AD_________________

Award Number: DAMD17-94-V-4015

TITLE: Advanced Medical Technology and Network Systems Research (Medical Vanguard Progarm)

PRINCIPAL INVESTIGATOR: Seong K. Mun, Ph.D.

CONTRACTING ORGANIZATION: Georgetown University
Washington, DC 20057

REPORT DATE: April 2001

TYPE OF REPORT: Final

PREPARED FOR: U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

DISTRIBUTION STATEMENT: Approved for Public Release;
Distribution Unlimited

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision unless so designated by other documentation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
April 2001

3. REPORT TYPE AND DATES COVERED
Final (31 Aug 94 - 31 Mar 01)

4. TITLE AND SUBTITLE
Advanced Medical Technology and Network Systems Research
(Medical Vanguard Program)

5. FUNDING NUMBERS
DAMD17-94-V-4015

6. AUTHOR(S)
Seong K. Mun, Ph.D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Georgetown University
Washington, DC 20057

E-Mail: muns@georgetown.edu

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

1. Diplomatic Telemedicine Network
The ISIS Center and TATRC have been working with the US Dept of State, Office of Medical Services, to establish a telemedicine network involving 5 US Embassies (Kenya, Tanzania, Cameroon, Haiti and Dominican Republic) and 2 clinics in Washington DC and Fort Lauderdale.

2. Telemedicine for Chronically Ill Patients
It has been shown that close monitoring of patients with diabetes can improve their blood sugar levels and thereby reduce complications due to Diabetes Mellitus. We have developed a web based tool that facilitates close monitoring of patients with diabetes by their care team as well as by themselves. This tool teaches patients to become more self sufficient in caring for their illness.

3. Telemedicine for Rehabilitation
Cognitive Behavioral Therapy (CBT) has been found to be efficacious in the treatment of people who need to manage multiple physical symptoms associated with the spectrum of illnesses known as Chronic Multi-symptom Illnesses (e.g., Fibromyalgia, Chronic Fatigue, and Gulf War Veterans Illnesses). CBT (normally conducted face-to-face and in a small group format) is known to reduce pain, increase function, and improve quality of life among these sufferers. Our goal is to test out possible ways to deliver CBT treatment (in small groups) at a distance using videoconferencing technology, with an adjunctive Web site for conveying the CBT material.

14. SUBJECT TERMS
Telemedicine, diabetes, data security

15. NUMBER OF PAGES
231

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	Unlimited

Table of Contents

This page left blank intentionally

Wireless Networks and "Universal Connectivity"

Duk-Woo Ro, PhD
Associate Professor of Radiology
Georgetown University
2115 Wisconsin Avenue, Suite #603
Washington, DC 20007
rod1@georgetown.edu

The emerging importance of wireless local area network (LAN) supported by IEEE 802.11 and wireless "universal connectivity" supported by Bluetooth will be emphasized in this course illustrating the current capabilities and limitations. The proliferation of mobile computing devices, including laptops, personal digital assistants (PDAs), and wearable computers, has created a demand for wireless personal area networks (PANs). PANs allow proximal devices to share information and resources. As these technologies develop over time, wireless devices and functionalities will have impact in the way radiology is practiced, and some examples of current and potential applications will be discussed. Security issues when accessing patient information over wireless devices also will be addressed in the course.

Outline:
(1) Types of wireless local area network
(2) Current bandwidth supported by IEEE 802.11
(3) Bluetooth and personal wireless area network
(4) B-to-B (building to building) wireless networking
(5) Making wireless environment secure
(6) Examples of current wireless application in radiology
(7) Potential applications in radiology practices as standards and protocols are further developed

Wireless LAN: IEEE 802.11

There are two types network based on IEEE 802.11: ad hoc and infrastructure. In the ad hoc network, computers are brought together to form a network "on the fly." There is no structure to the network, and usually each node communicates with every other node. In the second type of infrastructure wireless network, a fixed network of access points interfaced to a fixed-wired LAN is used to communicate with the mobile units. An example of such wireless infrastructure network is shown in Figure 1. When the mobile unit roams from one area to another or to a different service area, then a handover of the IP from one access point to the other is made. The physical layer of the network can use either direct sequence spectrum, frequency-hopping spread spectrum, or infrared (IR) pulse position modulation. The data rates can range from 1 Mbps–11Mbps and operate at 2.4–2.4835 GHz in spread-spectrum transmission and 300–428,0000 GHz for IR transmission. Devices operating at 5 GHz are being developed.

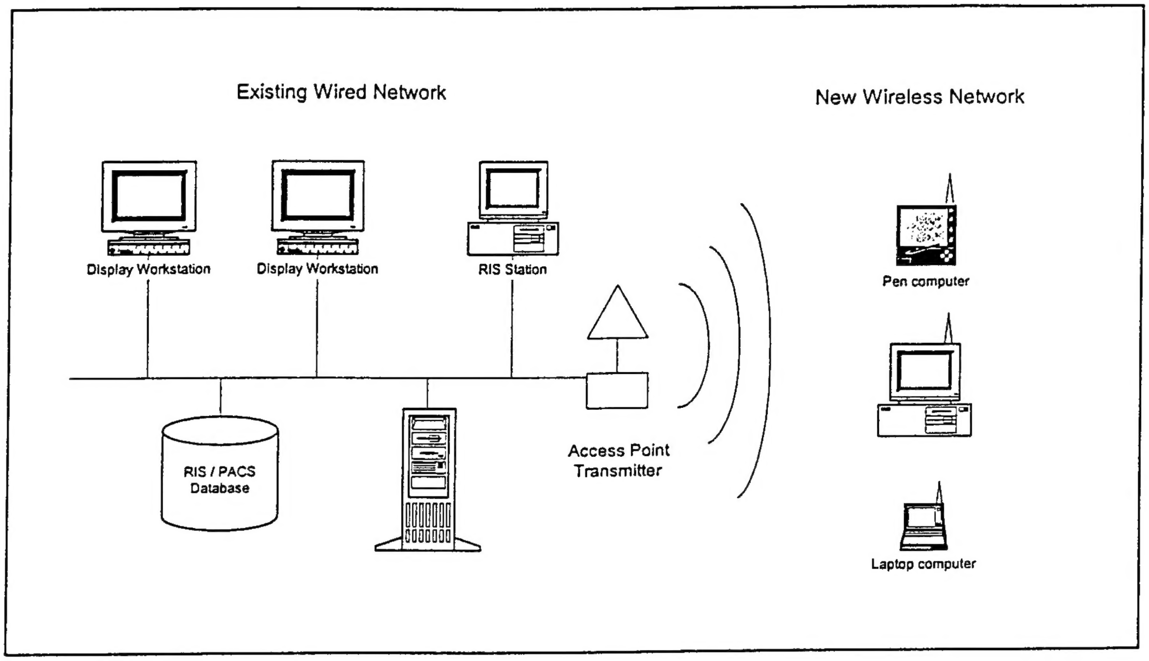


Figure 1: Integrating existing wired LAN used in PACS or RIS to wireless LAN

"Universal Connectivity": Bluetooth

Bluetooth wireless technology is a de facto standard, as well as a specification for small-form factor, low-cost, short-range radio links between mobile PCs, mobile phones, and other portable devices. It will enable users to connect a wide range of computing and telecommunications devices easily and without the need of cables. Piconets are established between devices and the host on an ad hoc basis for automatic and unconscious connections between devices. Currently, Bluetooth SIG (Special Interest Group) has defined USB, RS232 (serial cable), UART, and PC Card as alternatives for a Bluetooth module to be connected to a PC (host). This technology achieves its goal by embedding tiny, inexpensive, short-range transceivers into the mobile devices that are available today, either directly or through an adapter device such as a PC Card. The radio operates on the radio band, 2.4 GHz, and supports data speeds of up to 1 Mbps, as well as voice channels.

IEEE 802.11 and Bluetooth: ISM Broadcast Band

Some devices have Bluetooth technology, a low-power, low-range radio device for personal connectivity, alongside IEEE 802.11b LAN options. Recent concerns over the maturity of both wireless 802.11b LAN options and Bluetooth technologies, which operate on the same broadcast band (or the Industrial, Scientific and Medical ISM band), brought to light the fact that Bluetooth still has 2–5 years of development left and that 802.11b awaits two additional draft standards addressing the problems of data-transmission collisions with Bluetooth, and other performance issues.

Security

As HIPPA's data security measures are enforced in the health care environment, the methods used to perform wireless data transmission and authentication between devices and host to access patient data and information over public airwave will become increasingly important. Also, with the advent of wireless we will see the spread of viruses at a much faster rate. The Melissa virus, which spread via e-mail, took about 24 hours. In multilinked devices that make transactions via wireless, the spreading of virus from WAP phones, PDA, wireless LAN will be instantaneous. There will be days in the not-too-distant future when miniature firewalls and VPNs come between the Palm-type device and the gateway to block rogue infrared devices from getting your data. Things that you can do to protect your data on wireless devices include:

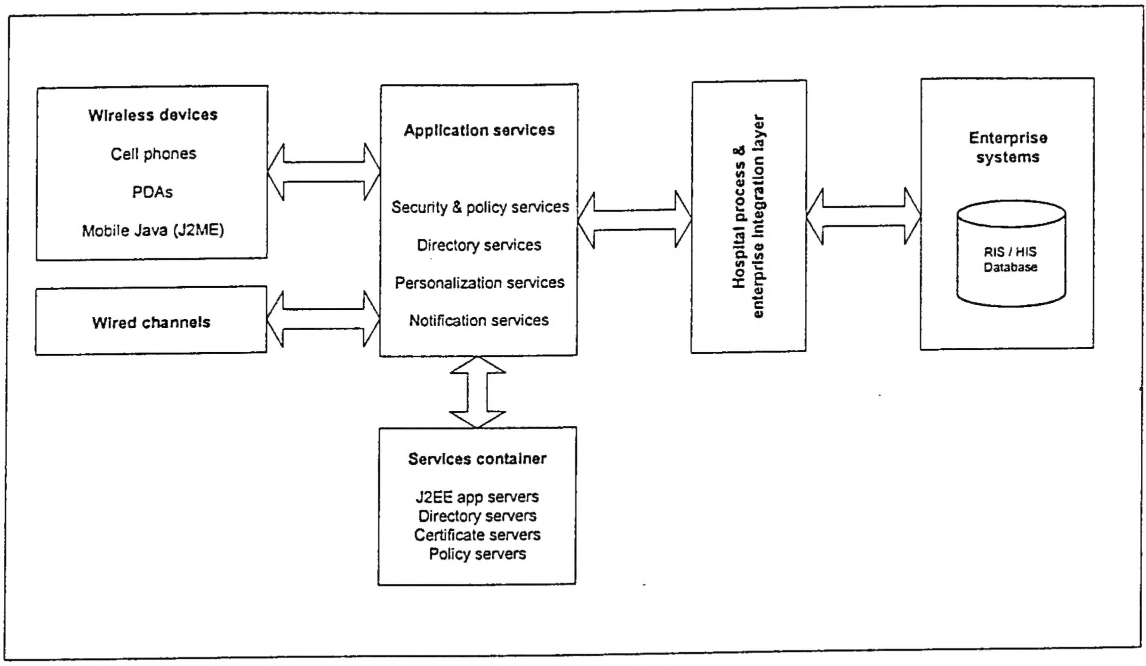


Figure 2: Security for the wireless and wired devices accessing patient information

1. The more network-centric solutions you design with the least amount of sensitive data residing in the handheld, the better off you are.
2. A server-type certificate built into the client so that the client authenticates the server before the password is used from the network to authenticate the client prevents spoofing, in which a user uploads sensitive data to what he thinks is his network server, but is not..
3. For most wireless networks, an additional layer of security must be put on top of the built-in security mechanism. In the industry, it is recognized that you cannot rely on GSM (Global System for Mobile communications) security alone. CDMA (Code Division Multiple Access) has a stronger security natively, and CDPD (cellular Digital Packet Data) typically need to run an application layer on top of their native security.

Web Resources

http://computer.org/students/looking/summer97/ieee802.htm: A short tutorial on wireless LANs and IEEE 802.11

http://www.bluetooth.com: The official site of Bluetooth standard and technology providing comprehensive documentations for industrial partners and developers alike for specifications, white papers and potential areas for future development.

This page left blank intentionally

MyCareTeam: A Disease Management Web Application

Ming-Jye T. Hu, Betty Levine, Adil Alaoui, Stephen Clement, Seong K. Mun
Georgetown University Medical Center, Washington DC
E-Mail: mingjye@isis.imac.georgetown.edu

Abstract

There has been an explosion of medical information and content on the World Wide Web in the past few years. More and more individuals use the WWW to find out about a disease or illness, to learn about possible treatments and cures, or to learn about new research on a given illness. MyCareTeam is an interactive Web application that utilizes Internet and computer technologies to provide interactive, customized care to patients with diabetes. It allows individuals with diabetes to better monitor their glucose levels, understand their lab values, realize the effect exercise and diet have on their disease, get educational information and most importantly to better communicate with their healthcare team on these issues.

Keywords

Internet, World Wide Web, disease management, diabetes

Introduction

While the Internet has been around for approximately 30 years, the vision of some of the founders of the Internet remain clear today : "... allowing computers to share information on research and development in scientific and military fields."[1] Today, it connects many independent networks spanning over 170 countries around the world.[2] When the World Wide Web (WWW) began in 1990, few suspected how successful it would become. Today, there are millions of websites with over one billion web pages. With all this information on the Web and all kinds of search engines available, people can easily find the information they want and exchange ideas and news.

In recent years, more and more individuals use the WWW to find out about a disease or illness, to learn about possible treatments and cures, or to learn about new research on a given illness. However, the interactive use of the WWW to manage chronic diseases, like diabetes, is still relatively new.

What is diabetes? Diabetes is a disease in which the body does not produce or properly use insulin, a hormone that is needed to convert sugar, starches and other food into energy needed for daily life. It is a serious and lifelong condition that affects about 16 million Americans, and over 5 million of these people are unaware that they have the disease. About 2,200 new cases are diagnosed every day in the United States. It can cause devastating complications, including blindness, heart disease, kidney disease, that often result in disability and death. [3] In 1996, diabetes was the seventh leading cause of death in the US in 1996. The American Diabetes Association estimated that the nation spends more than $98 billion every year on direct and indirect costs of diabetes. [4]

To avoid possible complications, patients with diabetes need close and continuous monitoring by themselves and a healthcare team. A diabetes patient who follows a required rigorous management regimen is able to lead a productive and satisfying life. However, due to the high demands of this regimen and the life-long nature of the disease, patients have a great deal of difficulty following their regimen.

MyCareTeam. We have developed a Web application that allows individuals with diabetes to better monitor their glucose levels, understand their lab values, realize the effect that exercise and diet has on their disease, and most importantly to better communicate with their healthcare team on all these issues. We focus on keeping the system simple and user-friendly for both patient and physician users. Through the application, we hope to improve patient compliance through education, prevent complications through fast and effective intervention, and provide continuing care of patients.

Methodology

Data Acquisition. Patients use an electronic device to record their blood glucose readings, the One Touch

Profile glucose meter from Johnson and Johnson. It can store a maximum of 250 glucose readings. An application run on the patient's computer uploads the glucose readings directly from a port on the glucose meter to the patient's PC through the serial port, and when an Internet connection is established, the patient sends the data to the secure central database. The application was designed to minimize the patients' input in the process of transferring data to the database.

Web Accessing. As patients and their healthcare team access the web site, they see a summary of the results of the most recent glucose readings, lab data, and other information deemed important to the care of the patients. We use automated analysis of the latest glucose levels to determine possible areas of concern (like number of hypoglycemic events and average blood glucose levels) that are identified by the endocrinologist. The site then drills down in the data to look for patterns in these alerts by day of the week or time of the day. This data is presented to the patient and healthcare team as they log into the web site. If the clinical data shows that problems are beginning, the computerized analysis of the data alerts the patient and healthcare team of the possible problems. Patient can also communicate with their healthcare team through data summary pages to provide comments regarding their latest glucose levels, and through email. On-line graphs of glucose levels over the course of a given period of time are presented to patients and their healthcare team.

Exercise is important to people with diabetes for controlling blood glucose levels. Therefore, patients are asked to log their exercise routines and provide comments for the healthcare team. Exercise can lower blood glucose, help the body use its food supply better, and help insulin work better.

Diabetes related educational materials and links to other diabetes web sites are provided to help patients understand their disease better and keep them informed of new research and clinical trials. A listserve is available for the participants on the site to communicate with each other, and is moderated by the clinical staff of the healthcare team.

Confidentiality and Security. We understand and respect the confidentiality of patient information. As long as the patients don't give out their login name and password, any confidential information that they send and receive on the Web site can only be seen by MyCareTeam staff members. Staff members include clinical and technical staff. Clinical staff view data to better monitor patients' care and technical staff view data in the course of their work to maintain and improve the web site.

In addition to the privacy policy, we have three layers of security implemented.

- **Access control.** All participants, including the patients and healthcare team, need a login name and password to get into the private side of the web site. For each patient login only information related to that individual is available. The care team can access only their patients' information.
- **Encryption.** All the communication between the patient computer and the web server is encrypted. Encryption prevents patient information from being intercepted.
- **Firewall.** A firewall is in place to provide an extra layer of security. A secure central database sits behind the firewall and is interfaced to a Web Server.

Results

While our clinical trial using MyCareTeam has not begun yet, our preliminary study connected 15 patients with type I diabetes to their endocrinologist using a point-to-point non-Internet line. Out of 15 patients, 10 transmitted their blood glucose data weekly to their Endocrinologist, an average of 25 times (biweekly) over one year. Glycemic control remained excellent for the duration of the study (HbA1C 6.1±0.86 at baseline, 7.1±0.75 at 12 months).[5]

The primary study proved that closely monitoring people with diabetes and frequent patient-physician communication and feedback can significantly lower the risk of complications of diabetes and avoid hospital and ER visits thus potentially increasing the quality of life and life expectancy of patients.

Discussion

Disease management programs offer an extraordinary opportunity for information technology to enhance the lives of patients, especially those patients who are alone or home bound," says John Osberg, president of Informed Partner LLP, a Marietta, Ga.-based health care consulting firm.[6] "I.T. presents real possibilities to increase the quality of care and significantly reduce the cost of care for these patients." [6] The 1993 Diabetes Control and Complications Trial demonstrated that patients with insulin-dependent diabetes mellitus reduce their risk of developing, or of worsening, diabetic eye disease - retinopathy, diabetic kidney damage - nephropathy, diabetic nerve disease – neuropathy by 50 – 75% when treated intensively. [7]

According to statistics from the Centers for Disease Control and Prevention, early detection and proper treatment of diabetes can prevent up to 90% of incidents of blindness, can reduce amputations by more than 50%, and reduce kidney disease and dialysis by over 50%. The total annual savings to the federal budget would exceed $2 billion.[3, 4, 8]

Traditional care of patients with diabetes include regularly scheduled visits to the doctor's office every 2 to 3 months. Often the data necessary to manage patients' blood glucose levels are inaccessible, making prevention and detection of problems difficult. MyCareTeam provides a way for patients to monitor their own condition, share information with their healthcare team, and get health education information immediately over the Internet. We propose that this will lead to patients better controlling their own condition and gaining an improved understand of how Diabetes affects them. Disease management programs have been shown to improve patients awareness of their disease and become more vigilant about maintaining their good health. The Internet is an ideal mechanism to deliver this service and provide more effective communications between patients and their healthcare team. It allows the healthcare team to respond quickly to a patient's changing health condition.

We do not expect to see the MyCareTeam Web site replace the standard of care in place today, but we do expect to find that it enhances compliance and adherence to clinical regimes and therefore can assist in achieving improved measurable health care outcomes. It follows then that if this is shown to be true, then one can expect that increased patient-healthcare team interactions and the early identification of potential problems may also reduce overall health costs.

Related Work

Associated with MyCareTeam is a similar site, MyKidneyTeam, designed to help patients with kidney disease who are on peritoneal dialysis (PD). These patients perform a form of dialysis at home instead of going to a dialysis center for hemodialysis. Patients enrolled in this project use the Baxter Healthcare HomeChoicePRO^{TM} dialysis machine for their home dialysis. HomeChoicePRO^{TM} comes with a modem that allows a member of the care team to dial into the device and download the stored dialysis data as well as patients' weight and blood pressure readings which are entered by the patient daily. The PD parameters retrieved is important to early detection and prevention of serious complications. This part of the project was funded under a National Library of Medicine contract.

Acknowledgments

This project was funded in part by the Department of Defense, grant number DAMD17-94-V-4015, and National Library of Medicine contract number # N01-LM-9-3537. The authors would like to thank both institutions for their continued support. We also would like to thank Christine Karakshian, Joyce Walter, Prakash Jha, Mason Miller, and Jun Choi for their continued help and support in the development of the MyCareTeam Web Site.

References

1. Howe, Walt A brief History of the Internet http://www0.delphi.com/navnet/faq/history.html#www, Apr. 2000.

2. Howe, Walt What is the Internet? http://www0.delphi.com/navnet/faq/Internet.html

3. National Diabetes Fact Sheet: National estimates and general information on diabetes in the United States. U.S. Department of Health and Human Services, Centers for Disease Control and Prevention. National Center for Chronic Disease Prevention and Health Promotion. Nov 1998.

4. Diabetes: A Serious Public Health Problem At-A-Glance 2000. U.S. Department of Health and Human Services, Centers for Disease Control and Prevention. 2000.

5. Adil Alaoui, Stephen Clement, Nassib Khanafer, Jeff Collman, Betty Levine, Seong K Mun. Diabetes Home Monitoring Project, *Proceedings of Pacific Medical Technology Symposium-PACMEDTek, Transcending Time, Distance and Structural Barriers, August 1998*, *Honolulu, Hawaii.* 258-261.

6. Greg Gillespie. Deploying an I.T. Cure for Chronic Diseases. *Health Data management*, 68-74, July 2000.

7. The Diabetes Control and Complications Trial Research Group: The effect of intensive treatment of diabetes on the development and progression of long-term complications in insulin-dependent diabetes mellitus. N Engl J Med 1993; 329:977-986

8. Diabetes Statistics. NIH Publication No. 99-3892, March 1999.

Reprinted from

Journal of High Speed Networks

Journal of High Speed Networks 9 (2000) 15–30
IOS Press

Telemedicine: challenges and opportunities

Sang-goo Lee [1], Seong K. Mun, Prakash Jha, Betty A. Levine and Duk-Woo Ro

Imaging Science and Information Systems (ISIS) Center, Department of Radiology,
Georgetown University Medical Center, Washington, DC 20007, USA
E-mail: {lee, mun, jhap, levine, ro}@isis.imac.georgetown.edu

IOS
Press

OHM
Ohmsha

JOURNAL OF HIGH SPEED NETWORKS

Aims and scope

The *Journal of High Speed Networks* will serve as an archive for papers describing original results of lasting significance in both the theory and practice of high speed networks. The Journal publishes contributed papers on original research, survey papers on topics of current interest, technical notes, and short communications to report progress on long-term projects. Submissions to the Journal will be refereed consistent with the review process of leading technical journals. The Journal is published quarterly.

The Journal encourages submissions on all aspects of high speed networking. The topics covered will include, but will not be limited to: the design and analysis of high speed networks; protocols for high speed communications; high speed LANs, MANs, and WANs; broadband ISDN and services; optical networks; control and management of high speed networks; high speed switches, interfaces and controllers; routing, flow control and congestion control in high speed networks; formal approaches to high speed protocol development; network management; multimedia applications; applications of high speed networks; experiences with operational high speed networks; multi-protocol label switching.

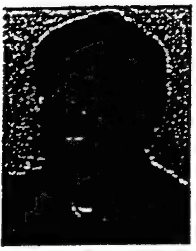
Published quarterly 0926-6801/00/$8.00 Printed in the Netherlands

Telemedicine: challenges and opportunities

Sang-goo Lee [1], Seong K. Mun, Prakash Jha, Betty A. Levine and Duk-Woo Ro

Imaging Science and Information Systems (ISIS) Center, Department of Radiology,
Georgetown University Medical Center, Washington, DC 20007, USA
E-mail: {lee, mun, jhap, levine, ro}@isis.imac.georgetown.edu

Abstract. Telemedicine is many things to many people. Only until a few years ago, telemedicine was equated to video teleconferencing between physicians, while nowadays, perhaps the most active area in telemedicine is the store-and-forward model. There is a big shift from private and dedicated modes of communications to connectivity through the Internet. Presented is a collection of applications that provide snapshots of this diversity. The key technical challenges identified from these experiences are connectivity and integration. Also, at issue are the evolution process through which a telemedicine application evolves and the ability to choose the right set of technology for the diverse type of telemedicine applications. With the projected improvements in speed and quality of the Internet, wireless communication, and personal computational devices, it is expected that various concepts of telemedicine will develop into standard practices in tomorrow's health care.



Sang-goo Lee received his Ph.D. and M.S. degrees in computer science from Northwestern University, Evanston, IL, in 1987 and 1990, respectively. He was a Research Engineer at EDS Research and Development, Troy, MI, and is currently an Associate Professor at the School of Computer Science and Engineering, Seoul National University, Seoul, Korea. This work was conducted while he was a Visiting Research Scholar at the Imaging Science and Information Systems Center, Georgetown University Medical Center, Washington, DC, between 1999 and 2000. His research areas are database systems, digital libraries, and medical informatics.

Seong K. Mun received his Ph.D. degree in 1979 from State University of New York, Albany, NY. He is the Director of the Imaging Science and Information Systems (ISIS) Center, Department of Radiology, Georgetown University Medical Center, Washington, DC. He is also the Director of Special Initiatives and Director of Medical Informatics for the Georgetown University Medical Center. He has founded the International Conference on Image Management and Communication System and has served as chair and member of numerous committees of national and international organizations on medical imaging, medical informatics, and telemedicine.

Prakash Jha received his M.D. in India from University of Rajasthan in 1989. After his residency in Pathology from University of Manitoba, Canada, in 1996, he completed his Masters in Public Health from George Washington University, Washington, DC. Dr. Jha was Quality Improvement Coordinator at George Washington University Health Plan. He is currently an Assistant Professor of Radiology and Clinical Director of ISIS at Georgetown University, Washington, DC. His areas of interest include preventive health, outcomes based disease management, and medical informatics.

[1] Currently on leave from School of Computer Science and Engineering, Seoul National University, Seoul, South Korea.

Betty A. Levine (M '96) has been with the Imaging Scence and Information Systems (ISIS) Center, Department of Radiology, Georgetown University Medical Center, Washington DC, since 1987. Ms. Levine currently manages many of the telemedicine projects within the ISIS Center. She is currently directing a web based Telemedicine for Chronic Illness project. Her other areas of expertise include digital imaging networks, systems integration, and information and imaging systems interfaces. She has designed and developed many interfaces that utilize the ACR-NEMA, DICOM 3.0, and HL-7 standards. She is one of two senior engineers responsible for the design, development, implementation, and installation of the Deployable Radiology (DEPRAD) network in Bosnia-Herzegovina, Hungary, and Germany.

Duk-Woo Ro received the M.S.E. and Ph.D. degrees in Biomedical Engineering from the University of Pennsylvania, Philadelphia, PA, in 1987 and 1990, respectively. He is currently an Associate Professor of Radiology at Georgetown University Medical Center, Washington, DC. Prior to joining Georgetown University, Dr. Ro served as the PACS Director of Samsung Medical Center, Seoul, Korea, and as a Research Assistant Professor at the Korea Academy of Industrial Technology, Seoul, Korea. His research areas include PACS, image management, and global health management.

1. Introduction

Telemedicine, in one form or another, has been practiced for over forty years. At the simplest level, a nurse providing clinical advice over the telephone is practicing telemedicine. Today, however, we think of telemedicine applications that employ advanced image and video as well as audio capabilities. These technologies can range from high-resolution still images (e.g., X-rays) to sophisticated interactive teleconferencing systems. Telemedicine now has the potential to make a difference in the lives of many Americans. For example, telemedicine can improve the delivery of health care in America by bringing a wider range of services such as radiology, mental health services, and dermatology to communities and individuals in under-served urban and rural areas. In remote rural areas, where the distance between a patient and a health professional can be hundreds of miles, telemedicine can mean access to health care where little had been available before. In emergency cases, this access can mean the difference between life and death. In particular, in those cases where fast medical response time and specialty care are needed, availability of telemedicine can be critical. In addition, telemedicine can also help attract and retain health professionals in rural areas by providing ongoing training and collaboration with other health professionals.

Cybermedicine, if defined as medicine in the Internet, is quite distinctive from the telemedicine as we know today, although there are overlapping issues, especially as the Internet can also be used (though limited) as a medium for telemedical applications. While the context in which telemedicine have been conceived until now focuses primarily on exchange of confidential clinical data with a limited number of participants, for the most part between patient and physician or between physician and physician, there is a global exchange of open, non-clinical information, mostly between patient and patient, sometimes between patient and physician, and between physician and physician. Telemedicine for the most part is applied to diagnostic and therapeutic medicine, while cybermedicine is applied to preventive medicine (prevent the occurrence of disease, for example by health education, as well as in the reduction of the consequences of disease, for example by information exchange among patients through newsgroups, websites, or via E-mail) and public health. With the improvement of Internet connectivity, these two applications will merge and become what can be called *e-medicine*. All the telemedicine applications may be practiced through the Internet including the interactive video and store-and-forward applications. For the purposes of this paper, we will adopt the Institute of Medicine's definition where 'telemedicine' refers to *the use of electronic information and communications technologies to provide and support clinical health care when distance separates the participants* [17].

Telemedicine can be divided into three areas: aid to decision-making, remote sensing, and collaborative arrangements for the real-time management of patients at a distance. As an aid to decision-making, telemedicine includes areas such as remote expert systems that contribute to patient diagnosis or the use of online databases in the actual practice of medicine. This aspect of telemedicine is the oldest in concept. Remote sensing consists of the transmittal of patient information, such as electrocardiographic (ECG) signals, X-rays, or patient records from a remote site to a collaborator at a distant site. It can also include the transmittal of grand rounds for medical education purposes or teleconferences for continuing education. Collaborative arrangements consist of using technology to actually allow one practitioner to observe and discuss symptoms and other aspects of cases with another practitioner whose patients are far away. Two-way workstations that provide smooth digital motion pictures have been integral to the long distance, real-time treatment of patients. As new technology is created and used effectively, collaborative arrangements are the future of telemedicine.

In the next section, we will discuss how telemedicine has evolved over time. In Section 3, a diverse collection of telemedicine applications are presented. A discussion on the technical issues based on these experiences is given in Section 4. We conclude in Section 5 with some outlooks of telemedicine in the future.

2. The emergence of telemedicine

The existence of telemedicine can be traced back to the first uses of the telephone. For example, in 1877, twenty-one local doctors built one of the first telephone exchanges to allow easier communication with the local drugstore. Although these early efforts fit the broad definition of telemedicine (use of telecommunications technologies to delivery health care), modern characterizations of telemedicine have occurred within the last thirty years.

Lovett and Bashshur [24] divided the development of telemedicine into three stages. The first stage was characterized by pioneering efforts with few public or private resources to support them. The second stage, between 1965 and 1973, was marked by deliberate efforts towards research and development and received short-term federal support. The third stage continued from 1973 through 1979 and involved evaluation by interdisciplinary teams with social scientists and specialists in medical care organization, planning, and delivery included for the first time. The Space Technology Applied to Rural Papago Advanced Healthcare (STARPAHC) program, a 20 year effort, marked the intersection and application of telecommunications technology expertise gained from the Space Program to the problem of delivering medical care to the Papago Indian reservation. This 3.3 million-dollar project advanced the understanding of how telemedicine applications could alleviate many of the access concerns related to healthcare delivery. Evaluations of these early telemedicine projects suggested that the technology was reasonably effective in transmitting the information necessary for most clinical uses and that patients were generally satisfied with their treatment [4,17].

Unfortunately, the telecommunications infrastructure of the 1970s (and prior) that was necessary to transmit high resolution images, video and audio signals was scarce and prohibitively expensive [1,2]. The newness of the technology by users and experimenters resulted in inefficiencies and was met with a general reluctance to adopt [1,12–14]. Funding agencies, in their haste to discern a cost effectiveness model in the face of escalating technology costs, pulled the support from these demonstration projects. Without government funding, the projects failed [1,2].

While many of the early attempts for telemedicine could not be sustained, there are some examples of highly successful programs using very simple technologies. One such example is the radio medical network in Alaska. In remote villages in Alaska, Health Aids trained to manage patient encounters following strict guidelines established by the Indian Health Service. They are authorized to administer care by the village doctors who are located in larger towns hundreds of miles away. At a given time of the day, the Health Aids make radio calls to the village doctors and review the patient encounters. The doctors can then instruct the Aids to deliver certain treatments or other follow up care. In serious situations, patients can be interviewed directly by the doctors. This system, though primitive, has been able to improve the quality of care throughout the remote villages in Alaska, illustrating how simple technologies can be useful in certain environments.

The 1990s have witnessed the culmination of a number of factors that support the resurgence of telemedicine applications. These factors include the national push for information super highways, advances in high-speed telecommunication, introduction of interactive video teleconference systems, and the growing interests in integrated healthcare systems.

A very significant recent event in telemedicine may be the introduction of video teleconferencing systems (VTC) [31] into the health care environment. These systems were originally developed to facilitate business meetings between people separated by long distance. As costs declined and quality improved, VTC soon captured the imagination of medical users and was implemented as a means of delivering health care. Teleradiology, although a form of telemedicine, could not be as readily launched for some years due to exorbitant costs of special equipment for high resolution and fine shades of gray images and massive data volume. The applications for interactive face-to-face consultations facilitated by VTC, however, transcended many clinical disciplines. Although not originally designed for health care applications, VTC systems were quickly integrated with medical peripherals such as electronic stethoscopes, endoscopic cameras, and other devices that provided additional diagnostic capabilities to telemedicine practitioners.

Telecommunication connections facilitate collaboration and partnership among distinct entities and foster the emergence of new forms of virtual organizations [32,37]. These virtual organizations are no longer defined or limited by geographic boundaries or physical distance, but are facilitated through complex, high-speed telecommunication connections that allow face-to-face and data exchanges. As virtual organizations, integrated healthcare organizations can function effectively across distance and time.

Telemedicine faces different challenges depending on the needs of various sectors in healthcare. Patients demand that telemedicine improve the quality of care and access to specialists. Provider organizations, such as hospitals, demand that telemedicine be capable of reducing the cost of care. To some, telemedicine may offer opportunities to reduce the operating cost by consolidating and streamlining management of multiple facilities. Physicians and other providers may see telemedicine as a means to improve their financial standing by attracting more patients to their services. Others however, may see telemedicine as a threat. The payers are concerned that indiscriminant use of telemedicine may increase the cost of care without any improved outcomes. Many technological advances in medicine help diagnose, treat and prevent illnesses and their roles are generally well defined, but the role of telemedicine is often unclear because it does not directly diagnose, treats, or prevent diseases.

3. Diversity of telemedicine

Telemedicine is many things to many people. Only until a few years ago, telemedicine was equated to VTC, while nowadays, perhaps the most active area in telemedicine is the store-and-forward model. There is a big shift from private and dedicated modes of communications to connectivity through the Internet. Table 1 shows a number of illustrative telemedicine applications, and the technologies by which they might reasonably be accomplished [15]. Presented in this section are a collection of applications that portray this diversity in telemedicine.

3.1. Deployable radiology

The United States military has always been an effective proponent of digital imaging and teleradiology. A teleradiology network makes military medicine requirements simpler by eliminating both the need to deploy radiologists and the use of X-ray films. X-ray film requirements include storage of new, unexposed films, storage, use, disposal of chemicals and water for processing, and storage of films and reports, all of which demand considerable amount of resources and logistics undertaking. The Imaging Science and Information Systems (ISIS) Center at Georgetown University Medical Center recently collaborated with the US Army in developing Deployable Radiology (DEPRAD), an off-the-shelf teleradiology network for the peace-keeping mission in Bosnia [22]. The network was part of Operation Primetime III [41]; a project to deploy advanced communications and medical equipment to provide state-of-the-art medical care to the 20 000 US troops stationed there. The network encompasses three major sites: the 212th Mobile Army Surgical Hospital (MASH) in Tuzla, Bosnia, the 67th Combat Support Hospital (CSH) in Taszar, Hungary, and the Landstuhl Regional Medical Center (LRMC) in Landstuhl, Germany.

At the MASH in Bosnia, a radiology local area network (LAN) had been installed which supports the following three modalities plus film digitization: computed radiography (CR), computed tomography (CT), and ultrasound

Table 1

Examples of telemedicine applications and the technologies that might be used

Technology: Telemedicine Application	Telephone/Radio	Facsimile	Email	Interactive Video	Store & Forward	Data Transmission	Real-Time Telemetry	Virtual Realit	Telerobotics
Informal "curbside" consult between providers	●								
Transmission of EEG or electrocardiogram data		●			●	●	●		
Real-time interactive orthopedic examination and consultation				●					
Transmission of diabetic patients' blood glucose data from home		●				●			
Asynchronous P -based dermatology consultation					●				
Psychiatric assessment of need for hospitalization	●			●					
Home health care services for hospice patients				●					
Transmission of physiologic data by EMT in an ambulance							●		
Interpreting a stroke patient's CT scan before administering TPA				●	●	●			
Consultation with a physician by physician assistant	●	●		●	●				
Home health care for persons with chronic conditions	●			●		●	●		
Patient education .	●		●	●					
Remote supervision of laparoscopic surgical procedures				●				●	
Performing remote laparoscopic surgery				●			●	●	●
Diagnosis of an astronaut's acute illness during space flight	●			●			●		
Trauma and emergency consultation for rural hospital staff	●			●	●				
Management of patients with drug-resistant tuberculosis			●		●				

(US). A schematic of the MASH configuration is shown in Fig. 1. The CSH configuration is quite similar. The LRMS installation was designed to receive images only from the MASH and CSH and display or print them as necessary. The clinical scenario is to acquire images using any of the three modalities listed above or by digitizing existing film. The images are then sent over a local area network to a Siemens workstation in the radiology for storage and viewing. Since there is typically not a radiologist at the MASH, the images are then transmitted to the CSH for primary diagnosis and archiving. Images can also be transferred to other display stations within the MASH depending on the patient location.

Several types of communication systems were used throughout the DEPRD network, which is shown in Fig. 2. A 10BaseT LAN was implemented to move images within the MASH and CSH. Wide area communications between LRMC and the MASH utilized microwave and satellite links. Images acquired at the MASH were sent via a microwave extension to a United States air base. The data were then relayed to Landstuhl via satellite connection. The communication between Landstuhl and the CSH was over E-1 lines (2.048 Mbps signaling rate) leased from the German and Hungarian telecommunication companies. Internet access was established at all sites.

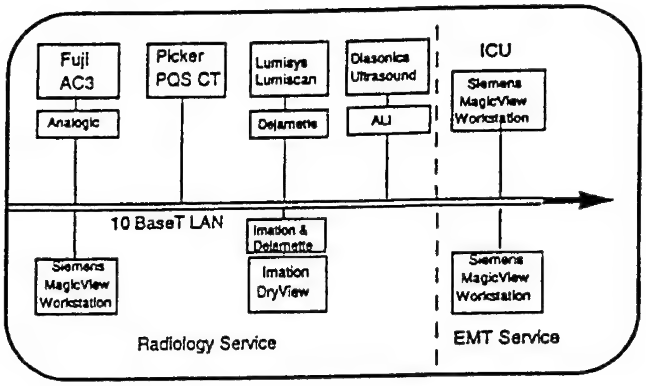


Fig. 1. DEPRAD local configuration.

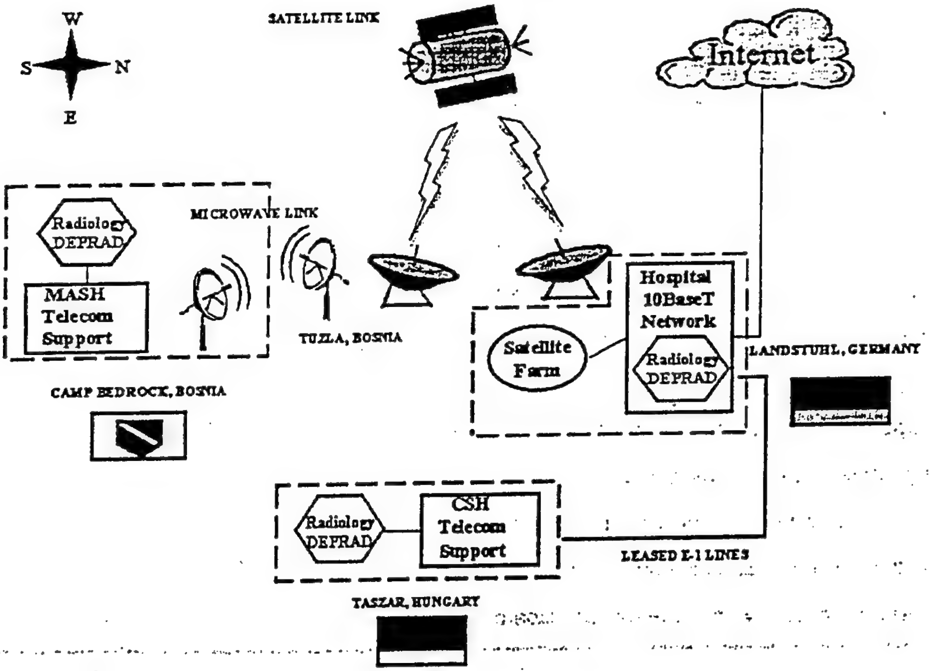


Fig. 2. DEPRAD communication diagram.

A number of devices were required to establish the filmless radiology and teleradiology capability that linked the three medical facilities. In order to connect all of the equipment in a clinically useful network, the Digital Imaging and Communication in Medicine (DICOM) 3.0 standard was required [3]. While DICOM is fast becoming the standard of choice by most medical imaging vendors, limitations of the standard were realized. Among the DICOM implementations encountered, none was connected without modification to configuration files, software changes, patches by vendors, or operational changes [23].

3.2. A multi-center digital MRI network

The Center for Neurogentic Diseases of Kennedy Krieger Research Institute (KKI) at Johns Hopkins University, Baltimore, Maryland, in collaboration with the ISIS Center at Georgetown University, is developing a global MRI

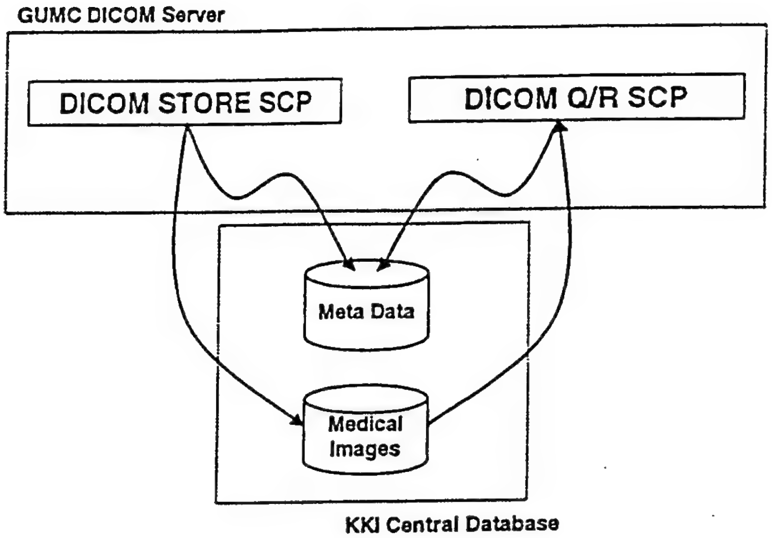


Fig. 3. DICOM server architecture.

network that allows participating sites to consult on adrenoleukodystrophy (ALD) magnetic resonance imaging (MRI) cases. Brain MRI and magnetic resonance spectroscopy (MRS) are the most sensitive indices for the evaluation of ALD therapies, but require the transmission of high quality images and the evaluation of these images by neuro-radiologists with extensive ALD experience. Due to the rareness of this disorder, this network is required to provide a sufficient number of patients for evaluating ALD therapies. This network will improve the ability of the participating institutions to evaluate ALD therapies.

Each participating site will electronically transfer MRI studies of ALD patients to the central clinical database at the KKI. The central database serves as a DICOM server, a storage-and-retrieval application that conforms to the DICOM standard for transmission of medical images (Fig. 3). The DICOM server provides the function of receiving and storing DICOM images as a DICOM Storage Service Class Provider (SCP). It will also respond to queries for the stored images as a DICOM Query/Retrieve (Q/R) SCP. The imaging modalities at the contributing sites are DICOM Storage Service Class Users (SCU), while workstations used by the radiologists to request the studies for review are DICOM Q/R SCU. Commands and data are exchanged between the provider and the users in the form of DICOM messages.

An important issue that needs to be addressed in transmitting and sharing patient data is patient confidentiality. Data received at the KKI will arrive with the patient identification information intact. Therefore, wherever possible, firewalls will be used to create virtual private networks (VPN) to protect the information being transmitted. Once data has been received, the identifying information will be stripped off and a system-generated identifier will be assigned. The central clinical database as well as the DICOM server will sit behind the firewall. While the DICOM protocol cannot pass directly through the firewall, due to limitations of current firewall protocols, a 'secure hole' will be opened in the firewall to allow the packets to pass through.

3.3. VTC based global patient care

The Office of Medical Services (MED) based in Washington, DC, operates, administers, and manages a worldwide health care program for employees and their families serving abroad with the US Department of State and other associated US Federal agencies. The clinical staff assigned to the MED's Health Unit in Nairobi, Kenya, have presented extraordinary demands on MED Washington's health care services and program planning as a result of the Embassy bombing on August 7, 1998. To address this demand, in part, the Department of State, in cooperation with the US Army Medical Research and Materiel Command (USAMRMC), established a telemedicine platform linking the Department of State Health Unit in Nairobi, Kenya, to MED Washington in October of 1998. In addition to the telemedicine platform linkage, the Division of Medical Informatics of the State Department must sustain and expand telemedicine services to the Health Unit Nairobi.

The ISIS Center at Georgetown University Medical Center has been involved in the efforts with the responsibilities of project management support, engineering and technical operations support, and analysis and evaluation of the telemedicine services between the Health Unit at the US Embassy in Nairobi and the MED Washington.

Initially, the preferred mode of consultation was VTC between Nairobi and Washington primarily for clinical consultation, and Nairobi and the ISIS Center for technical support and project management. Regular biweekly meetings via VTC between the three sites were established. However, because of the high communications cost required for VTC that was provided via ISDN connectivity using satellite communication, the mode has shifted almost entirely to the more cost-effective store-and-forward model. An off-the-shelf telemedicine application, in conjunction with digital capture devices such as X-ray digitizer, dermascope, ENT scope, opthalmoscope, and digital video camcorder was used to carry out physical examinations of patients and to send the acquired exams over a secured Department of State's network. Although all communications are through a secured private network owned by the Department of State for obvious security reasons, the technologies employed are Internet compliant, such as HTTP, TCP/IP, and SMTP.

The major challenge in this project was not so much in the technical areas but in training and education; getting people in different parts of the world to adapt to a new mode of health care procedure.

3.4. Home health monitoring over the Internet

Telemedicine is no exception to being greatly influenced by the Internet. With the Internet connecting millions of households and virtually all institutions, it makes perfect sense to deliver health care services to patients' homes over the Internet. A pilot project aimed at close monitoring of patients with chronic diseases is currently underway at the ISIS Center at Georgetown University Medical Center. The project currently focuses on two types of patients; patients with end stage renal disease performing Peritoneal Dialysis (PD) at home and those with diabetes. The primary goal of the system is to assist in the close monitoring of patients in their homes. The second goal is to provide relevant information to the patient so that they may become more self-sufficient, better informed about their disease and their health, and more compliant in administering their prescriptions.

The system aims to provide a single easy to use Web interface to all users. The patients will routinely upload their glucose readings, PD data, or other relevant information to a central database server. All data from monitoring devices will be uploaded automatically from the devices whenever the user logs on the Web site and connects the device to his/her computer. The patients can view previously entered data, their progress, and prescriptions through user friendly Web interfaces. The physicians need more complicated views and functions, some of which are readily available in commercial products. In order not to reinvent the wheel and to allow physicians to use the software they are already accustomed to, a couple of patient management software products are being integrated to the system. The challenge to this approach is in integrating the databases used by the different systems. A consolidated data model has been defined which serves as the data model for the central database and also as the reference model to which each of the other databases has to be translated into.

Smart agents are being developed and implemented to perform certain critical tasks including checking parameters and ensuring that they are within target ranges, reminding patients of upcoming appointments and prescriptions, and presenting new information and educational materials relevant to the current situation.

3.5. DBMS based medical conferencing

Most conventional teleconferencing systems work in a mode called 'copy-and-synchronize', in which the conference material must be prepared prior to the conference time and copied into local disk of every site [21,33]. In such setups, data are not directly retrieved from database at the time of a conference. Also, saving the conference result (proceedings) had to be done manually. A system designed and implemented at Seoul National University

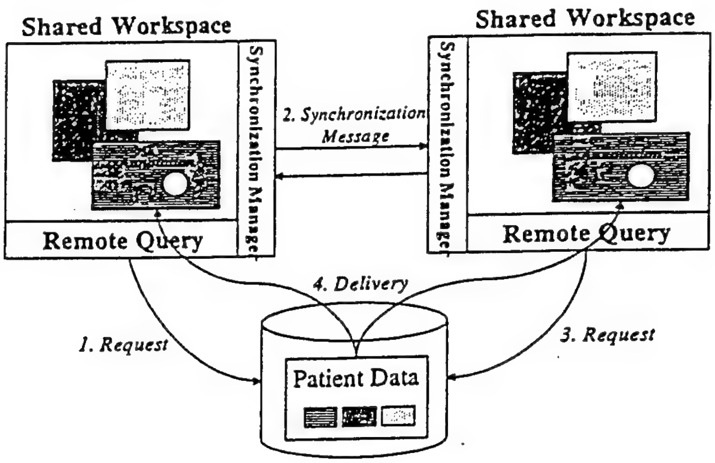


Fig. 4. Synchronization in DBMS based teleconference.

Hospital, Seoul, Korea, aims to build a teleconferencing system that is tightly integrated with the multimedia hospital database [20]. By integrating the teleconferencing functions into the database client application, users can conduct teleconference sessions using the same database interface they would use routinely to retrieve patient data.

Figure 4 shows a conceptual depiction of the way this system works. The Shared Workspace is the database interface augmented with functions for teleconferencing, such as proceedings control and annotation. The teleconferencing system synchronizes all windows events such as movement of the mouse, push of a button, and input from the keyboard. This synchronization translates into sending the same requests (or queries) to the database server, thus resulting in synchronized presentation of data.

The following design objectives that were pursued in this project are relevant to most medical teleconferencing applications.

- A teleconferencing system must be directly integrated with the existing medical database application so that patient information needed for a conference, whether previously expected or not, may be dynamically retrieved during the time of a conference. The system must also be able to store and maintain the result (proceedings) of a conference.
- The teleconferencing system must be more than an interconnection of different applications. The system must provide an integrated shared workspace that allows participants to organize the various forms of conference related data and to present the materials systematically for better conferencing. The workspace should be flexible enough to meet various conference contexts for different medical communities.
- A teleconferencing system must support a unified view of a patient's record that mimics a real-world patient chart. Since most conferences are held for a single patient's case, it is important to have the system ready to present all information that is related to that patient's case. Through the workspace, we can provide an integrated view of various patient data [34].

Database access and workspace synchronization are carried out over the Internet. The system also included a separate VTC setup through which the physicians talked and watched each other while manipulating the database together. However, the physicians quickly abondoned the interactive video and were comfortable with only the telephone to complement the conference session. This meant abondoning the ability to send real time visual images captured during conference, but the users did not see much added benefit that would warrant the cost and hassle accompanied in setting up a VTC session.

4. Technical issues

4.1. Telemedicine applications and technologies used

Table 2 shows the different technologies employed by the telemedicine applications presented in the previous section. Voice communication, including telephone, is a basic necessity for all the applications. In all the situations where Internet connection was available, including those where Internet was not the primary mode of connection, emails were so prevalent that not using them made little sense. Interactive video is obviously a good feature to have, yet the demanding cost makes the store-and-forward model more widely accepted in these cases. The Data Transmission column indicates whether data from monitoring devices were actively captured and transmitted in the application. In VTC applications, there is the need to synchronize presentation of data and motions in the user interface. As the Internet becomes available to more people and organizations, we see a shift from doctor-to-doctor teleconsultations over private networks to patient care telemedicine over the Internet.

4.2. Connectivity

A typical VTC application requires 2–4 ISDN lines (256–512 kbps) to a full T1 line (1.544 Mbps) capacity, depending on the quality of video. Figure 5 shows the different bandwidth requirements for different modes of communications. With the rates as high as they currently are, telecommunications costs represent one of the biggest portions of the operational cost of telemedicine programs. Although bandwidth requirements are decreasing as technology advances, interactive-video-level connectivity is not the type of bandwidth that an institution can afford to reserve for a handful of applications. More often than not we witness a telemedicine program being modified to exclude or significantly reduce the interactive video features that were the main theme in the initial stages of the program.

The VTC-based Global Health Project presented in Section 3.3 is an example where the VTC feature, which was central to the concept of the project, was all but abandoned in the later stage. Setting up sessions across different international time zones was a difficult task to begin with, but the high communication cost was the biggest factor influencing the change.

Table 2
Telemedicine applications and the technologies used

Technology: **Telemedicine Application**	Telephone/Radio	Email	Interactive Video	Store & Forward	Data Transmission	Real-Time Sync	Connectivity[1]	Participants[2]
Deployable Radiology	●			●	●		P	D
Multicenter Digital MRI Network	●	●		●	●		I	D
Global Patient Care	●	●	●	●		●	P	D
Home Health Monitoring	●	●		●	●		I	P
DBMS Based Teleconferencing	●	●	●		●	●	I	D

[1] Private network (P) or Internet (I)
[2] Doctor-to-doctor (D) or doctor-to-patient (P)

The DBMS based teleconferencing system in Section 3.5 is another example. In this application, all participants were within the same time zone, eliminating the time difference factor. The deciding factor in this case was the hassle involved in setting up the VTC. The communications and device requirements for the VTC are such that it is not economically possible to make every room VTC-ready. The physicians would rather sit in their own offices and engage in teleconferences with only their PCs and telephones rather than move to the VTC-ready conference room. Another factor is that the majority of the cases that physicians were interested in discussing with their colleagues were cases that had already been extensively reviewed locally. Most of the relevant tests and images have been taken and are available in the database, which can be browsed in a synchronized manner. In such cases, interactive video is no more than an expensive 'video phone' showing the picture of the other party.

It would be wrong, however, to conclude that the merits of interactive video is marginal in telemedicine. On the contrary, a careful examination of the above projects shows that abandoning VTC has been a compromise between the goals set in the beginning of the project and the cost and efforts involved in providing interactive video. A discussion or a consultation is likely to be more productive when the parties meet face-to-face, and if this is not possible, VTC is obviously the next best option. More importantly, there are situations where it is vital to see ultrasounds or ECGs as they are administered at the remote site. So, the problem is not that telemedicine can do without interactive video but rather it is too inconvenient and expensive. Communications cost is still too high for most VTC applications to be cost effective. Most VTC devices, such as the Coder/Decoders (Codecs), are still too expensive to be a part of an average 'multimedia-enabled' PC for the home and office.

With the trend towards physician-to-patient home health care [11,43], connectivity at homes is becoming ever more important for telemedicine. The Home Health Monitoring project described in Section 3.4 is an example of the growing number of applications in this direction. Anyone with a modem and a telephone line can have Internet access through an Internet service provider (ISP). However, most telemedicine services providing interactive physician-to-patient interactions require more speed and reliability than can be offered by this mode. Connections over ISDN and cable modems are two of the few modes that can provide higher speed and reliability. But, as Grigsby, et al. [15] observe, advanced telecommunications infrastructure is not available for many rural areas. Even for those areas where the necessary transmission media are available, they may be prohibitively expensive. There is also evidence of disparity between the rural areas in rates for similar level of transmissions. This is a serious situation given that the most effective use of home health telemedicine would be in the rural areas.

In order to realize the true potential of telemedicine, high-speed connectivity should be available in each room of a hospital and each household. One should be able to plug in any medical device to these outlets and feed images and videos to any designated PC or node on a local network or the Internet.

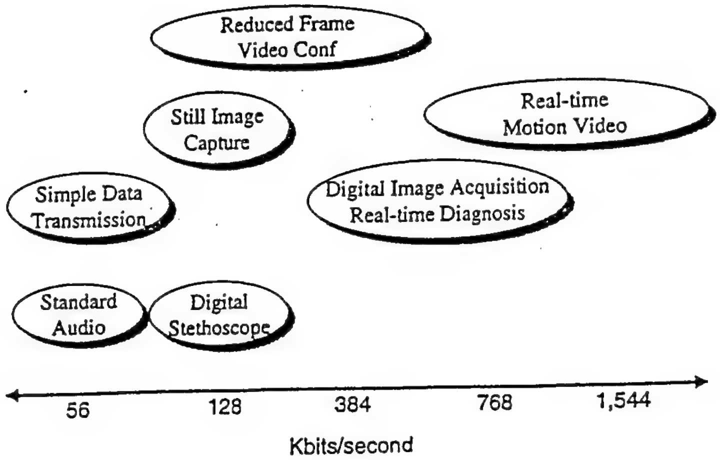


Fig. 5. Bandwidth requirements.

4.3. Integration

Telemedicine is an integrated application by nature. One must address the integration of image display, data presentation, human computer interface, data storage and management, network, communications, electronic and medical devices, etc. The software modules defined in a telemedicine system will likely include patient demographics data browser and editor, examination results display, image viewer and annotator, and teleconferencing. Some of these features are available in one commercial system or another, but it is very difficult to extract and then integrate these features from disparate systems that we end up inventing the wheel again. This has been a particular difficulty in the project described in Section 3.4 where two commercial systems for physicians had to be integrated with the newly developed patient system. Furthermore, the configuration of the integrated components, as well as the components themselves, must be dynamically changeable in order to cope effectively with different types of diseases, different stages of a patient, and the new and changing specifications of medical devices. Thus, as much as any integrated information system, a telemedicine system stands to gain enormously from software engineering technologies that provide a better way to reuse software codes, integrate functionality, and modify on the fly. Component-based software engineering technology and object request broker (ORB) architectures such as CORBA and CORBA-MED [16,18] seem to be efforts in the right direction, but their practical merits are yet to be seen.

Another dimension in the integration issue is data. A typical patient's record will consist of demographics, physical exams, X-ray exams, blood and urine exams, and dietary and exercise information, all from different laboratories and clinics. A patient's record kept in his/her primary care institution should be readily available when the patient checks into an emergency room in another state. This is a classical database integration problem with syntactic and semantic disparities to be resolved. The medical community was early to identify this problem and has been trying to address it [6,10,35]. Telemedicine simply magnifies and brings the problem to the forefront.

Software and hardware integration issues cannot be addressed without adopting standards. Standards are required for almost all aspects of telemedicine such as EMR (Electronic Medical Records) and their exchange, device-to-device transmission, real time collaboration and constraints, software interface and integration, and teleconference functions such as synchronization and web annotation.

4.4. Framework of telemedicine development

As the examples in the previous section indicate, the term telemedicine alone does not adequately describe the specifics of any one application. Telemedicine applications face different barriers and challenges based on the goals of the project, the technologies incorporated, and the context of the users. The field of telemedicine is facing many of the dilemmas that confront any new field that is created through technological innovation. The technology must evolve through its own development, while creating applications that help, to then define the technology's own future growth. In this way, the technology helps to define the applications, while at the same time, the applications help to define the technology. This technology development process involves the following four basic stages [27].

Stage 1 – Development of Basic Technological Capabilities

Telemedicine will require a new array of technologies in sensors, imaging, computer-controlled devices, communications, voice driven systems; complex and intelligent database and network technologies. During Stage 1 we see the development of new types of technology involved in various stages of the health care delivery process. These technologies may involve information capturing, information transmission, or interpretation. As these technologies develop, innovative practitioners develop ways in which the technology can be incorporated into their practice.

Stage 2 – Development of Relevant Applications

Stage 2 describes the initial development of applications to meet the capabilities of new technologies. As these technologies begin to be used within various health care applications, practitioners can envision ways in which the innovation can be adopted on a grander scale. As more research is developed to support the use of specific telemedicine applications, greater support within specific medical disciplines and federal agencies will evolve. In this stage, the acceptability of the technology for specific applications can be validated and clinical efficacy demonstrated.

Stage 3 – The Integration of Technical Applications within a Complex Environment

Telemedicine applications realize the third stage of the technology development process as concerns about reimbursement, licensure, credentialing, and standards continue to be debated at the national level. Our laws, credentialing systems, and reimbursement mechanisms were not created with a virtual environment in mind. Unfortunately, instead of recognizing the uniqueness offered by virtual space, our licensing, credentialing and reimbursement systems have tended to ignore this new environment. Instead, we force our physical world laws into virtual space. Studies suggest that the most common specialties using telemedicine as a means of providing care were mental health, emergency/triage, cardiology, dermatology, and surgery respectively [13]. This suggests that these five specialties are more amenable to telemedicine applications than others, although another research [25] suggested that telemedicine use might be more practitioner specific than specialty specific. In either case, adopting a new technology into the way of practicing medicine is a major undertaking that deserves more recognition than is currently given within the medical and engineering community.

Stage 4 – The Transformation of the Operating Environment

Stage 4 describes the transformation of the environment to incorporate the new telemedicine applications. The complex issues of the environment, coupled with the demands of the applications create a new focus on the needs that are present and the solutions that are available. As technologies become integrated within specific applications, new technologies develop that can improve the efficiencies and quality of the existing system. At this point the cycle begins again. In some cases, the telemedicine innovations will evolve within an existing health care delivery environment. In other cases, telemedicine innovations will expand the environment to new locations. An example of this expansion can be seen in the use of telemedicine within the home.

4.5. Determining the technical requirements of a telemedicine application

Many technical approaches exist for providing telemedicine services. Choosing the appropriate equipment for a telemedicine project requires careful analysis. The following questions help guide the technical analysis [29].

1. *What technical functionality does the project require*? The needs assessment drives the answers to this question. Not all telemedicine projects require video conferencing. Most technical services come in a variety of flavors. Choices increase daily but are constrained by the services a project proposes to deliver.
2. *What telecommunications bandwidth does the project require*? Making a selection of equipment to meet a project's needs usually establishes a minimum requirement for bandwidth. The relatively slow rate of image transmission over the Internet yields choppy, poor resolution images unsuitable for clinical diagnosis, while the bandwidth may be acceptable for home health monitoring applications (see Fig. 5).
3. *May equipment be purchased off the shelf or does it require custom development*? As the market for telemedicine products has developed, conventional, off the shelf products have become increasingly available for many telemedicine applications. Moreover, standard products such as video conferencing equipment or personal computers compose segments of telemedicine networks even though not specifically designed for medical use.
4. *Is the technology known or must it be learned*? The users in a telemedicine project must develop expertise in using the equipment and services. All projects should include training for prospective users but should also evaluate the relative complexity of proposed technology as a factor in the likelihood of successful use.
5. *Does the project require new infrastructure or technical capability*? Many telemedicine projects begin as freestanding efforts that require installing dedicated or specialized communications infrastructure. As organizational information systems develop and Internet based applications emerge, telemedicine projects will use common infrastructure at different levels of the global communications network.

6. *Is technical support available in-house or must it be purchased*? Few telemedicine applications are 'plug-and-play', thus requiring technical support at some level. Projects vary in their support requirements and in the availability of suitable personnel in the organization.

5. Conclusion

The Internet is here to stay. We expect the future to bring us a 'ubiquitous Internet' where everyone is connected to everyone everywhere. The successful efforts in advanced projects such as the Internet2 [40] and Next Generation Internet [8] indicate that the future of Internet promises to be faster and more reliable. For telemedicine, this means more options to more people. It is expected that the majority of telemedicine applications of the future will operate over the Internet instead of private networks. Technologies such as Virtual Private Network (VPN) will make peer-to-peer type telemedicine over the Internet less risky. Homes in certain parts of the world are already experiencing high speed Internet connection through digital subscriber lines (DSL) and cable modems, albeit at high prices. The advance in compression and communication technology, coupled with the fierce competition within the communication industry, will bring down communication charges. This will allow bandwidth hungry features such as interactive video to become affordable basic features of almost all telemedicine applications.

Already people in Japan and Netherlands are enjoying wireless digital phone services with data communication rates of 28 kbps or higher [9]. Wireless data communications at the personal level will be prevalent in the near future. It is perceivable that laptops, PDAs, and other mobile devices will be our main tools for Internet access. Mobile access standards such as the Wireless Application Protocol (WAP) [42] will enable such a transition and mobile satellite communications will allow global reach of voice and data services. This will open a new dimension of options for telemedicine applications. Paramedics will be able to care for patients at the site of an emergency with (almost) full connection to the hospital systems and resident physicians, and true uninterrupted patient monitoring and care can be realized around the clock. Pilot projects at the Mayo Foundation, Rochester, MN, and St. Elizabeth Hospital, Appleton, WI, have already successfully demonstrated the concepts using two way pagers [36].

Coupled with wireless communications, intelligent and convenient end-user devices will bring true mobility and interactional constancy. Wearable computers are expected to play important roles in future telemedicine. The goals of a wearable computer are to be mobile, to augment reality (not to replace nor to simulate), and to provide context sensitivity [7]. One application would be a nurse wearing a special pair of eyeglasses, where specific information about the prescription and treatment for the patient he/she is seeing will be presented either on the glasses or through the ear-piece. Another example is of an intelligent wristwatch that will constantly monitor the vital signs of a patient and alarm him/her of any concerns over the portable stereo headphones. There will be no more manual uploading or typing of the measurements from the patient monitoring devices.

We also envision medical devices being able to talk to each other, without a web of cables connecting them, by use of technologies such as embedded wireless where a high-speed wireless transceiver is embedded in every processor chip [30]. For example, without any hookups or cables, endoscopic images can be fed into a desktop computer, which in turn sends the data over a wireless network to a consulting physician. The consulting physician would be able to control the various monitoring devices that are set up in a remote operation room

Advanced software technology, such as mobile agent technology, will evolve to meet the needs of large complicated systems. Mobile agents are active objects that can migrate autonomously from computer (device) to computer to perform computations on behalf of their owners, either users or programs [19]. The mobile agent paradigm brings the computation where the information is stored or is generated in cases of real time monitoring. One application of this technology is in dynamic customization of patient devices. This ability to upgrade and reprogram user devices over the network should drastically reduce the maintenance cost of doctor-to-patient type telemedicine applications. A mobile device deployed need not be programmed to cope with all possible scenarios but only be able to accept mobile agents as necessary. The mobile agent paradigm is only one of a list of innovations that we expect will provide a means to build dynamic and adaptive software systems that are maintainable.

Home health care is already one of the most important areas of telemedicine. Researchers argue [43] that the home health care environment must, first and foremost, be easy and comfortable. Their applications must be unobtrusive and, preferably, transparent. The devices and technology must be easy to use. It is indeed possible to design, manufacture, install, and implement medical and health care technologies which are simpler and easier to use. The home must remain a home, and not look like an intensive care unit or an emergency room. Product design should be using a 'consumer model' rather than a 'medical model'. Appropriate and affordable communication technologies and networks are vital to home health care. The need and challenge is to seamlessly connect home health care monitors, sensors, and devices to these communication systems and thus to the various professional care providers.

Telemedicine is expected to enjoy a 40% growth in the next 10 years and by 2010, telemedicine will represent 15% of total health care activities [38]. Advances in telecommunication and network technology will bring closer the virtual society, and telemedicine will play an essential role in health care in this newly defined society. There are exciting challenges and opportunities in exploiting available technologies and in shaping the future of technology. With continued efforts in this dynamic and blended field of health care and advanced technology, telemedicine will loose meaning as a separate field of study as its concepts and applications become standard medical practices, at which point it will have achieved its final objectives.

Acknowledgements

This work was supported in part by the Department of Defense under contract DAMD17-94-V4015. Sang-goo Lee's work was supported in part by the Korea Research Foundation's Support for Faculty Research Abroad.

References

[1] A. Allen and D. Allen, Telemedicine programs: 2nd annual review reveals doubling of programs in a year, *Telemedicine Today* 3 (1995), 10–16.

[2] A. Allen and M.L. Scarbrough, Third annual program review, *Telemedicine Today* 4 (1996), 10–38.

[3] American College of Radiology, National Electrical Manufacturers Association, *Digital Imaging and Communications in Medicine (DICOM): Version 3.0 Standard*, ACR-NEMA Committee, Working Group VI, Washington, DC, 1993.

[4] R.L. Bashshur, Critical issues in telemedicine, *Telemedicine Journal* 3 (1997), 113–126.

[5] R. Bashshur, J. Sanders and G. Shannon, eds, *Telemedicine: Theory and Practice*, Charles C. Thomas Publisher, Springfield, IL, 1997.

[6] G.W. Beeler, Jr., On the Rim: The Making of HL7's Reference Information Model, *MD Computing* 16(6) 1999, 27–29.

[7] M. Billinghurst and T. Starner, Wearable devices; new ways to manage information, *IEEE Computer* 32 (1999), 57–64.

[8] CCIC, *Next Generation Internet Initiative*, National Coordination Office for Computing, Information, and Communications, http://www.ngi.gov, 1998.

[9] C. Chandler, In Japan, the Internet without the PC, *Washington Post*, February 8, 2000.

[10] R.S. Dick and E.B. Steen, eds, *The Computer-Based Patient Record, An Essential Technology for Health Care*, Institute of Medicine, National Academy Press, Washington, DC, 1991.

[11] A. Goldberg, Tele-home healthcare on call: Trends leading to the return of the house call, *Telemedicine Today* 5 (1997), 14–15.

[12] B. Grigsby, Report on US Telemedicine Activity, Association of Telemedicine Service Providers, Portland, OR, 1997.

[13] B. Grigsby and A. Allen, Fourth annual telemedicine program review, *Telemedicine Today* 5 (1997), 30–42.

[14] J. Grigsby, Telemedicine Policy: Coverage and Payment, in: *Analysis of Expansion of Access to Care through Use of Telemedicine and Mobile Health Services*, Center for Health Policy Research, Denver, CO, 1995.

[15] J. Grigsby et al., Health Care Financing Administration: Draft Report to Congress on Telemedicine, Center for Health Services and Policy Research, University of Colorado Health Sciences Center, Denver, CO, 1999.

[16] J.J. Held, C.A.T. Susch and A. Golshan, What does the future hold for distributed computing, *StandardView* 6 (1998), 17–21.

[17] Institute of Medicine, *Telemedicine: A Guide to Assessing Telecommunications in Health Care*, M.J. Field, ed., National Academy Press, Washington, DC, 1996.

[18] V. Jagannagthan et al., Objects in healthcare – Focus on standards, *StandardView* 6 (1998), 22–26.

[19] K. Kavi, J.C. Browne and A. Tripathi, Outlook on networks: experimentation to harness the power of the Internet, *IEEE Computer* 32 (1999), 33.

[20] H. Kim, E. Park, S. Lee and Y. Shin, Collaborative workspace for multimedia medical conferencing, in: *Proceedings of the 9th World Congress on Medical Informatics (MedInfo)*, 1998, pp. 322–326.

[21] L. Kleinholz and M. Ohly, Multimedia medical conferencing: design and experience in the BERMED project, in: *IEEE Conferencing*, 1994, pp. 255–264.

[22] B.A. Levine, K. Cleary and S.K. Mun, Deployable teleradiology: Bosnia and beyond, *IEEE Transactions on Information Technology in Biomedicine* 2 (1998), 30–34.

[23] B.A. Levine, K. Cleary, G.S. Norton and S.K. Mun, Experience implementing a DICOM 3.0 Multivendor Teleradiology Network, *Telemedicine Journal* 4 (1998), 167–176.

[24] J. Lovett and R. Bashshur, Telemedicine in the USA, *Telecommunications Policy* (1979), 3–14.

[25] H. Mekhjian, J.W. Turner, M. Gailiun and T. McCain, Patient evaluation of telemedicine consultations: A matter of context, *Journal of Telehealth and Telecare* (2000) (in press).

[26] S.K. Mun, M. Freedman and K. Rajiv, The revolutionary use of imaging modalities requires companion advances in management of films and data: IMAC system for radiology, *IEEE Engineering in Medicine and Biology* (1993), 70–80.

[27] S.K. Mun and J.W. Turner, Telemedicine: Emerging e-medicine, *Annual Review of Biomedical Engineering* 1 (1999), 589–610.

[28] S.K. Mun et al., Experiences in implementation, clinical acceptance and operations of comprehensive radiology networks, *SPIE Medical Imaging III* 1093 (1989), 194–201.

[29] S.K. Mun et al., *Georgetown Telemedicine Guide*, Telemedicine Working Group, Georgetown University Medical Center, 1998.

[30] C. Partridge, Viewpoint: Embedded wireless connects Net to all and all to Net, *IEEE Spectrum* 36 (1999), 38.

[31] E. Rosen, *Personal Videoconferencing*, Manning Publication, New York, 1996.

[32] R.M. Satava, Virtual reality and telepresence for military medicine, *Annals of the Academy of Medicine of Singapore* 26 (1997), 118–120.

[33] E. Schooler, Conferencing and collaborative computing, *Multimedia System* 4 (1996), 210–225.

[34] E. Shortliffe et al., Collaborative medical informatics research using the Internet and the World Wide Web, in: *Proceedings of 1996 AMIA Annual Fall Symposium*, 1996, pp. 125–129.

[35] K.A. Spackman, Terminology Convergence: SNOMED gets a boost, *MD Computing* 16(5) (1999), 23–25.

[36] L. Stammer, TELECOM 2000, *Healthcare Informatics*, http://www.healthcare-informatics/issues/2000/01_00/cover.htm, 2000.

[37] P. Taylor, A survey of research in telemedicine: telemedicine services, *Journal of Telemedicine and Telecare* 4 (1998), 63–71.

[38] Telemedicine To Grow 40% Annually Over Next 10 Years, *Telemedicine Today*, http://telemedtoday.com/website99/news_items.htm, 1999.

[39] J.W. Turner and C. Peterson, Organizational telecompetence: Creating the virtual organization, in: *Telemedicine: Practicing in the Information Age*, S. Viegas and K. Dunn, eds, Lippincott-Raven, New York, 1998, pp. 41–48.

[40] UCAID, *Internet2*, University Corporation for Advanced Internet Development, http://www.internet2.edu, 1999.

[41] USAMRMC, *Primetime III Task Force, Operation Plan #1*, Unclassified Staffing Document, U.S. Army Medical Research Material Command, Fort Detrick, MD, 1996.

[42] WAP, Wireless Application Protocol, *Wireless Internet Today*, WAP Forum, http://www.wapforum.org/what/WAP_white_pages.pdf, 1999.

[43] J. Winters, ed., Report of the Workshop on Home Care Technologies for the 21st Century, Catholic University of America, http://www.hctr.be.cua.edu/HCTWorkshop/, 1999.

JOURNAL OF HIGH SPEED NETWORKS

Subscription information
The *Journal of High Speed Networks* (ISSN 0926-6801) is published in one volume of four issues a year. The subscription price for 2000 (Volume 9) is NLG 550 + NLG 44 p.h. = NLG 594 (US$ 297). The Dutch guilder price is definitive. The US dollar price is subject to exchange-rate fluctuations and is given only as a guide. 6% VAT is applicable for certain customers in the EC Countries. Subscriptions are accepted on a prepaid basis only, unless different terms have been previously agreed upon. Personal subscription rates and conditions, if applicable, are available upon request from the Publisher. Subscription orders can be entered only by calendar year (Jan.–Dec.) and should be sent to the Subscription Department of IOS Press, or to your usual subscription agent. Postage and handling charges include printed airmail delivery to countries outside Europe. Claims for missing issues must be made within six months of our publication (mailing) date, otherwise such claims cannot be honoured free of charge.

For individual members of ACM SIGCOM a personal member price will apply. Please contact the publisher for further details.

Instructions to authors
For detailed instructions please refer to our website on the Internet, www.iospress.nl.

Submission of manuscripts: Authors are requested to submit 5 copies of their manuscript as well as a floppy disk containing the electronic files of the paper to the Editor-in-Chief. **It is important that the file on disk and the printout are identical.**

Preparation of manuscripts:

1. Manuscripts must be written in English. Authors whose native language is not English are recommended to seek the advice of a native English speaker, if possible, before submitting their manuscripts.
2. Manuscripts should be typed on one side of the paper only, with wide margins and double spacing throughout. For the electronic file of the text you may use any standard word processor. Do not use page layout software and do not send PostScript files of the text.
3. The title page should contain (i) a title, (ii) author's name(s), (iii) affiliation(s), (iv) an abstract, (v) a complete *correspondence address*, including a telephone number, a fax number, and an e-mail address.
4. Each *table* should be provided on a separate sheet. Tables should not be included in the text.
5. *Figure captions* should be provided all together on a separate sheet.
6. Each *illustration* should be provided on a separate sheet. Illustrations should not be included in the text. The *original* drawings (no photocopies) are required. Electronic files of illustrations should preferably be formatted in Encapsulated PostScript Format.
7. *Footnotes* should be kept to a minimum, and they should be provided all together on a separate sheet.
8. *References* should be listed alphabetically in the following style:

   [1] D.S. Ahn and M.J. Lee, Optimal buffer allocation in ATM switches by effective cell loss, *J. High Speed Networks* 6 (1997), 247–262.

   [2] F.P. Kelly, *Reversibility and Stochastic Networks*, Wiley, New York, 1985.

   [3] D. Peleg and E. Upfal, A tradeoff between space and efficiency for routing tables, in: *20th ACM Symposium on the Theory of Computing*, 1988, pp. 43–52.

Proofs: The corresponding author is asked to check the galley proofs. Corrections other than printer's errors, however, should be avoided. Costs arising from such corrections will be charged to the authors.

Offprints: For each contribution the corresponding author will receive 25 offprints and one copy of the issue free of charge. An order form for additional offprints will be provided along with the galley proofs.

Copyright: Authors submitting a manuscript do so on the understanding that if their paper is accepted for publication, copyright in the article, including the right to reproduce the article in all forms and media, shall be assigned exclusively to the Publisher.

Publisher
IOS Press
Nieuwe Hemweg 6B
1013 BG Amsterdam
The Netherlands

Tel.: +31 20 688 33 55
Fax: +31 20 620 34 19

E-mail:
Subscription Department: order@iospress.nl
Advertising Department: market@iospress.nl
Desk Editorial Department: editorial@iospress.nl

Internet:
www.iospress.nl

Presented at IEEE November 2000 and published in the proceedings

Development of a Secure Medical Research Environment

Adil Alaoui, MS, Betty Levine, MS, Kevin Cleary, PhD, Seong K. Mun, PhD
Imaging Science and Information Systems (ISIS) Center
Department of Radiology, Georgetown University Medical Center, Washington, DC
Email: alaoui@isis.imac.georgetown.edu

Abstract

The confidentiality of medical information, including patient data security, is an increasingly important issue in today's health care environment. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) [1] requires the Department of Health and Human Services to create specific rules for managing the security and privacy of computer-based patient medical records. In November 1999, the Department of Health and Human Services implemented the privacy requirements of the HIPAA proposal to improve the effectiveness of public and private health programs by protecting individually identifiable health information.

In this paper we will give a brief description of some widely used security measures. We will also address the steps that were taken at the Imaging Science and Information Systems (ISIS) Center at Georgetown University to secure our research environment and the patient medical information used within the network, and describe our efforts to become more HIPAA compliant. The paper concludes with some clinical applications.

Keywords: Firewall, Virtual Private Network (VPN), Security, Encryption, Medical

Significance

The Imaging Science and Information Systems (ISIS) Center, Department of Radiology, Georgetown University, conducts research in applications of advanced computing and telecommunications technology applied to healthcare. In its capacity as an important civilian research laboratory with many Department of Defense grants and contracts, the ISIS Center has established a reputation for technical sophistication and organizational effectiveness through projects such as DIN-PACS (Digital Imaging Network Picture Archiving and Communications—the prototype and technical specifications for the DOD filmless radiology system which was the groundwork for the military project known as MDIS (Medical Diagnostic Imaging System)), Project DEPRAD (Deployable Radiology—a digital imaging teleradiology network built in support of the US troops in Bosnia-Herzegovina), and digital mammography (a proof of concept project and working model of adapting computed radiography technology to digital mammography). The ISIS Center also successfully competes for extramural funding from other government agencies including the National Institutes of Health and the National Science Foundation in the areas of image processing, computer-aided diagnosis, telemedicine, and image-guided therapy.

The ISIS Center faces major changes in its research environment. On the one hand, many projects acquire, manipulate and archive patient identifiable information on the ISIS Center local area network (LAN). This includes data from clinical trials for government and commercial funding agencies that are subject to Food and Drug Administration rules and regulations. On the other hand, investigators, physicians, and patients increasingly require remote access to such data using dial-up and web-based technologies. Whereas the ISIS Center has not historically faced major data security problems in its connections with untrusted networks, remote access requirements led to the development of a plan for managing the security and confidentiality of patient identifiable information on its LAN. The ISIS Center's approach to data security functions to protect patient data and to demonstrate how research involving patient data may be accomplished in a secure environment.

Primer on Security Options

Levels of Security

As in all academic, research, and commercial sectors, the Internet has become a vital mechanism in healthcare. Within the healthcare community, many physicians, researchers, and patients use the Internet to gather medical information. In addition, more and more patients are gaining access to their clinical data over the Internet. However, with increased ease of use and access to confidential information comes increased threats and vulnerabilities. Some of the threats that are of concern to healthcare professionals include unauthorized access, hacker attacks, virus infections, e-mail spamming, and address spoofing.

To address these risks there are a number of solutions and techniques that can be applied. The next section will discuss some of the more popular techniques available to secure a network and its data from the above-mentioned risks and threats.

Firewalls

A firewall [2] is a first line of defense against unauthorized attacks on the network. It controls access to a trusted network from outside users while allowing inside users access to the Internet and the outside world. It forces all connections to and from the untrusted network to pass through and obey all policies set at the firewall. A good firewall will achieve a delicate balance between desirable and undesirable data accessibility. A firewall can operate at different Open Systems Interface (OSI) layers and can be configured with multiple proxies to minimize compromising the users inside the firewall while remaining transparent. There are three types of firewalls:

1. Packet filter gateways are firewalls that operate at the lower level of the OSI model. A packet filter only checks for destination IP addresses and port numbers before granting access to the trusted network.
2. Circuit-level gateways are like packet filters except that they operate at a different level of the OSI protocol stack. Unlike most packet filters, connections passing through a circuit-level gateway appear to the remote machine as if they originated from the firewall. This is very useful for hiding information about protected networks.
3. Application level gateways are the most secure of the three firewall types mentioned here. Application level gateways function at the highest level of the OSI model, the application layer. These systems support strong user authentication and are data and application aware.

Acquiring and installing a firewall is just one piece of the security puzzle. Besides firewalls there are different security measures that can minimize threats and vulnerabilities. These other measures will now be discussed.

PKI

Public Key Infrastructure uses a pair of "keys"—public and private—to encrypt and decrypt messages. All messages and data sent using PKI are encrypted. The messages can only be decrypted by using the private key.

The two "keys" in a key pair use a sophisticated mathematical algorithm. When one key performs a certain function (such as encrypting an electronic message), only its corresponding key can complement that function (and decrypt the message) and in the process authenticate the sender and the integrity of the message.

In public key cryptography (the process that PKI supports), a key pair is used to encrypt and decrypt messages sent electronically over unsecured paths. It is this mathematical relationship that gives public key cryptography its power to provide for confidentiality, authentication, data integrity, and for access control for open highly scalable applications such as those needed and used in healthcare applications.

Access Controls and Authentication

Other than the basic login name and password combinations, there are different authentication methods used to increase security and access control to a network. Organizations can select one or more methods of authentication, most suitable for their applications. One of the most popular authentication methods is SecureID because it provides strong authentication and does not requires special readers or hardware. It uses a "token" to access the system. Other emerging authentication methods include Biometrics readers such as fingerprint readers, iris scanners, facial imaging devices, hand geometry readers, and voice readers. These provide an extra level of security and access control.

Virtual Private Networks

Virtual Private Networks (VPNs) are an emerging technology. They provide reliable low cost protection and privacy for organizations compared to the use of leased lines. All messages and data transferred over a VPN are encrypted.

A VPN creates a secure environment to access the Internet and exchange information and data. VPNs can be deployed to protect two networks or single workstations connected a secured network. With a VPN, remote users get connected to the trusted network as if they were on the same network. The Internet Key Exchange protocol (IKE) is used to authenticate, negotiate and manage the encrypted traffic.

ISIS Center Firewall

Steps Toward Security

In order for the ISIS Center to establish a secure network, the acquisition and implementation of a firewall started in 1998. A risk and needs assessment was undertaken to identify the potential risks to the network and weigh them against the threats of attack, loss of data, etc. Questionnaires were circulated to all researchers to determine the systems and communications/network protocols used within the ISIS Center and at remote sites that collaborate with the ISIS Center. All this information led to the creation of a comprehensive request for proposal (RFP). Vendors were asked to respond to specific user questions as well as being told what the expectations were of the vendor and/or firewall product.

All ISIS Staff evaluated vendor responses independently, and SecureMethods, Inc. (formally DynCorp) was selected to install and configure a Gauntlet firewall. SecureMethods worked with ISIS Center personnel to define security protocols and determine the appropriate firewall configuration. It was important to coordinate with and keep all ISIS staff members informed as the firewall could potentially impact their use of network services. Finally, installation and testing was scheduled over a weekend. During this time, access to the Internet and the outside world was limited.

Multiple system tests were performed to validate the configuration and operation of the firewall. Changes were made when user expectations were not met or when important tasks could not be carried out because of firewall settings. Each project was analyzed and tested to ensure that a mechanism was in place to allow the project to continue to operate with the firewall installed. The maintenance of the firewall and modification to the configuration is an ongoing task.

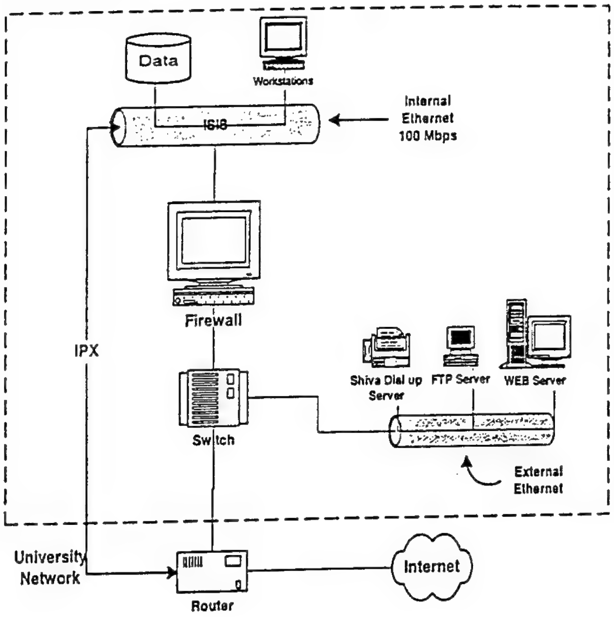


Figure 1. ISIS System Architecture

System Architecture

The major components of the ISIS network are shown in Figure 1 and include the Gauntlet firewall, a Cisco switch, and a router. The Gauntlet version 4.2 firewall is installed on a Micron PC running the Unix BSD 3.1 operating system with 128 MB RAM and a 10 gigabyte hard drive. The PC has 2 network cards: one connected to the outside untrusted network and the other connected to the ISIS LAN (trusted network).

As shown in the diagram the Cisco switch (Catalyst 5509) separates the ISIS network into two segments: internal (trusted) and external (untrusted). The Cisco switch also provides 100 megabits per second (Mbps) internal network speed.

All access to the ISIS network is through the firewall, except for the IPX protocol (Novell Protocol) which is routed around the firewall. IPX is not supported by the firewall and is considered a minimal security risk. To remotely access the internal network, registered users are authenticated by the firewall using a password generated by remote authentication software on the user's computer. Patient identifiable data, an email server, and data not meant for the general public are stored inside the trusted network. Our Web server, FTP server, and Shiva dial-up server are on the external Ethernet.

Gauntlet Firewall

The Gauntlet Firewall is a hybrid firewall operating as an application gateway and as a circuit gateway. Table 1 lists some of the important application proxies to the ISIS Center.

Proxy	Authentication	Extras
HTTP	Yes	Active X, Java, URL Filtering, Cyber Patrol
SSL	No	
SMTP	Yes	Virus Scan, Limit Size, Anti-Relay, Anti-Spam
POP3	Yes	
FTP	Yes	Transparent, Content Scanning
SQL	No	
Netmeeting	No	
Plug Proxy	No	Can be customized and configured to any port

Table 1. Gauntlet Proxies used at the ISIS Center

One limitation we found with the firewall is the lack of commercially available DICOM or IPX proxies. At the time of selection of the Gauntlet, there were no commercially available firewalls that contained these proxies. Both of these are important messaging protocols used within our environment.

To work around these limitations, a "secure hole" is opened in the firewall using a packet screening mechanism that allows communication between two known computers for known protocols and port numbers. A plug proxy can also be configured for any application allowing transport through a defined port. While the packet screening mechanism and plug proxy worked well for the DICOM protocol, IPX data still has to be routed around the firewall.

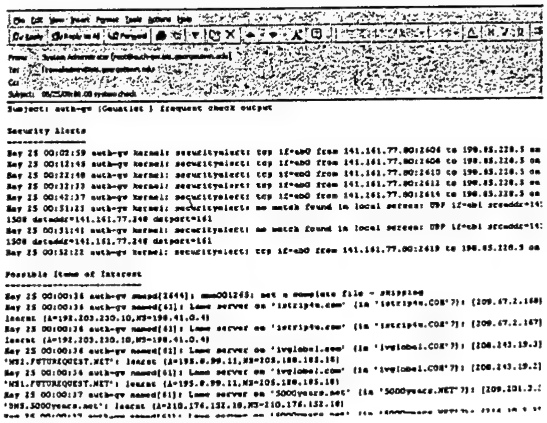
Management

The Gauntlet Firewall manager is the primary tool used for managing the firewall. It has a secure graphical interface accessible from authorized computers on the trusted network and allows remote workstations access to the firewall configuration.

Since the firewall administrator needs to be constantly aware of possible attacks, the reporting capabilities of Gauntlet are very useful, helpful and informative in this aspect. The firewall reporting and alerting features [3] are customizable and configurable to provide:

- Frequency Reports
- Types of Alerts
- Message Log
- Email Alerts

The reporting module of the Gauntlet also allows for logging and monitoring all failed processes, failed access attempts, packets that failed to pass the filter, and activities contrary to firewall configuration. Figure 2 shows an email message automatically sent from the firewall to the administrator warning of possible security violations.



From: System Administrator [root@auth-gw.isis.georgetown.edu]
To: firewalladmin@isis.georgetown.edu
Cc:
Subject: 05/25/00 00.00 system check

```
Subject: auth-gw (Gauntlet ) frequent check output

Security Alerts
---------------
May 25 00:02:59 auth-gw kernel: securityalert: tcp if=ab0 from 141.161.77.80:2606 to 198.85.220.5 on
May 25 00:12:45 auth-gw kernel: securityalert: tcp if=ab0 from 141.161.77.80:2606 to 198.85.220.5 on
May 25 00:22:40 auth-gw kernel: securityalert: tcp if=ab0 from 141.161.77.80:2610 to 198.85.220.5 on
May 25 00:32:33 auth-gw kernel: securityalert: tcp if=ab0 from 141.161.77.80:2612 to 198.85.220.5 on
May 25 00:42:37 auth-gw kernel: securityalert: tcp if=ab0 from 141.161.77.80:2614 to 198.85.220.5 on
May 25 00:51:23 auth-gw kernel: securityalert: no match found in local screen: UDP if=ab1 srcaddr=14:
1508 dstaddr=141.161.77.248 dstport=161
May 25 00:51:41 auth-gw kernel: securityalert: no match found in local screen: UDP if=ab1 srcaddr=14:
1508 dstaddr=141.161.77.248 dstport=161
May 25 00:52:22 auth-gw kernel: securityalert: tcp if=ab0 from 141.161.77.80:2619 to 198.85.220.5 on

Possible Items of Interest
--------------------------
May 25 00:00:16 auth-gw smapd[2444]: sma001265: not a complete file - skipping
May 25 00:00:36 auth-gw named[61]: Lame server on 'istrip4u.com' (in 'istrip4u.COM'?): [209.67.2.168]
learnt (A=192.203.230.10,NS=198.41.0.4)
May 25 00:00:36 auth-gw named[61]: Lame server on 'istrip4u.com' (in 'istrip4u.COM'?): [209.67.2.167]
learnt (A=192.203.230.10,NS=198.41.0.4)
May 25 00:00:36 auth-gw named[61]: Lame server on 'ivglobal.com' (in 'ivglobal.COM'?): [208.243.19.2]
'NS2.FUTUREQUEST.NET': learnt (A=195.8.99.11,NS=205.188.185.18)
May 25 00:00:36 auth-gw named[61]: Lame server on 'ivglobal.com' (in 'ivglobal.COM'?): [208.243.19.2]
'NS1.FUTUREQUEST.NET': learnt (A=195.8.99.11,NS=205.188.185.18)
May 25 00:00:37 auth-gw named[61]: Lame server on '5000years.net' (in '5000years.NET'?): [209.201.3.:
'DNS.5000years.net': learnt (A=210.176.152.10,NS=210.176.152.10)
```

Figure 2. Firewall Alert Email Example

Clinical Applications

With the firewall in place and configured to ISIS Center specifications and policies, we are able to securely use our systems to acquire and store not only research data but also patient information. Some examples of clinical applications at the ISIS Center that require secure data transfer are described below.

MyCareTeam

This is an interactive Web Site developed at the ISIS Center to give patients with diabetes and kidney disease access to their daily clinical data and to securely communicate and exchange medical information with their healthcare team. Diabetes patients connect to a secure Web site over the Internet using encryption and upload their daily blood glucose readings to the database which sits behind the firewall.

For patients with kidney disease, a point-to-point modem connection is established between the Peritoneal Dialysis (PD) machine in the patient's home and a secure database application at the ISIS Center. The data is securely uploaded to the database through the Web application. The patients can then access their daily PD data from the Web site. In designing the site, the HIPAA requirements for ensuring the protection of the privacy of medical information were taken into account [4].

To provide secure access to the data, the firewall was configured to allow traffic between the Web server (external Ethernet in Figure 1) and the Database server within the trusted Network (internal Ethernet in Figure 1). A Secure Socket Layer (SSL) connection is established with all pages in the Web site that transfer confidential data. 128-bit encryption is used.

Multi-Center Clinical Trial

A digital network for transferring magnetic resonance images (MRI) between multiple clinical institutions, the ISIS Center, and the Kennedy Krieger Institute in Baltimore, Maryland is under development under a National Library of Medicine contract. The purpose of the network is to develop a database of patients with a rare neurological disorder called ALD or Adrenoleukodystrophy. The purpose of the network is to facilitate clinical trials of new therapies or treatments. The secure transmission and storage of the MRI data is required.

While the firewall protects the data that sits behind it, other mechanisms were implemented to ensure no loss of data, no unauthorized access to the data, and to preserve the confidentiality of the patient data. First, VPNs are established between contributing clinical sites and the central database whenever possible. VPN client software is provided to contributing sites if a VPN server is not available at their institution. Similarly, patient names and unique identifiers are masked as soon as the data enters the database. This not only preserves the confidentiality of the patient data, but also blinds the researchers to the therapy the patient may be on when evaluating their MRI. Finally, the DICOM standard requires that the contributing site be known to the receiving system before the receiving system will accept its data. Similarly, sites that query the DICOM database, must be known and approved within the DICOM Query/Retrieve server before data are sent out.

Visualization

As part of a project in computer aided surgery, the ISIS Center often has a need to exchange DICOM images with clinical departments at the hospital or other research groups. One example of this need is related to our work with the Interventional Radiology group at Georgetown University Medical Center. We provide engineering support and systems integration assistance for a mobile CT scanner. The scanner is used during interventional radiography cases to obtain a series of axial images, which can then be reconstructed into a three-dimensional display for visualization purposes. Since the engineers working on this project are situated at our research group, we need to transfer the CT images from the hospital to the ISIS Center located 1 mile away. This image transfer is done using the DICOM protocol, and requires appropriately configuring the firewall as discussed earlier.

Conclusion

Now that the firewall has been installed, ISIS Center network administrators are able to restrict access to the internal network, monitor all transactions to and from the local area network, and securely exchange patient information and images with different institutions using the Internet. While changes to existing network architecture and operating environment were required, the transition to a secure environment went relatively smoothly. Participation and cooperation by all group members was critical towards minimizing inconveniences. The costs associated with the firewall implementation are moderate, but some dedication by the network administrator is required. We anticipate that such systems will become more common in the medical field as requirements for secure medical data become more widespread.

Acknowledgements

This work was supported by the U.S. Army under grants DAMD17-96-2-6004 and DAMD17-99-1-9022 and by The National Library of Medicine under contract NO1-LM-6-3544.

The authors would like to thank Albert Green Jr., Jeffrey Collmann, Ph.D., and Marion Meissner, MS, for their contributions to this article and the firewall installation.

References

1) Notice of Proposed Rule Making for Standards for Privacy of Individually Identifiable Health Information, Federal Register [NPRM] published November 3, 1999 http://aspe.hhs.gov/admnsimp/nprm/pvclist.htm, accessed August 2000.
2) M. Goncalves, "Firewalls Complete," McGraw-Hill, 1998.
3) Network Associates University "Implementing a Firewall using Gauntlet for Unix" [TNS-201-UNX]
4) Securing Electronic Information in HealthCare Organizations, http://www.verisign.com/rsc/wp/healthcare/healthcare.html, accessed August 2000.

Diabetes Home Monitoring Project

Adil Alaoui, MS.*, Stephen Clement, M.D., Nassib Khanafer, MS., Jeff Collmann, Ph.D.,
Betty Levine, MS. and Seong Ki Mun, Ph.D.
ISIS Center, Department of Radiology
Georgetown University Medical Center.
*E-mail: alaoui@isis.imac.georgetown.edu

Abstract

Objective: To study the feasibility of remotely monitoring people with diabetes using low-cost technology.
Methods: Randomly chosen people with type I diabetes will transmit their diabetes-related data to their physician at Georgetown University Medical Center on a weekly basis by using a personal computer. The physician will analyze it. Then, he will contact the patient every week to make safe adjustments to their diet, exercise plan, and insulin dosage to prevent different kinds of diseases.
Findings: Based on the data received the physician at the Endocrinology Department was able to early correct blood glucose levels for many patients enrolled in the program and prevent many possible clinical complications.
Conclusion: This preliminary study indicates that monitoring people closely with diabetes, frequent patient-physician communication, and feed-back utilizing a low-cost technology can significantly lower the risk of getting diseases. This project helps patients avoid costly short and long-term hospitalizations and ER visits. Also, it increases the quality of life and life expectancy.

Introduction

A successful management of diabetes depends on maintaining the blood glucose values within acceptable ranges. The Diabetes Home Monitoring Project enables the patient to clearly understand the disease and the physician. The physician in the Endocrinology Department at Georgetown University Medical Center will follow his/her patients' blood glucose level variation on a weekly basis to determine the patient's health conditions and changes over time. The purpose of this project is to remotely monitor patients who were previously diagnosed with type I diabetes using an electronic device to gather blood glucose levels and transmit them electronically to their physician in the Endocrinology Department of GUMC.
Each patient is supplied with a One touch Profile glucose meter by Johnson and Johnson and an IBM compatible personal computer with "in Touch" Diabetes Management Software by Lifescan Johnson and Johnson.

Technical Description

The One Touch Profile meter is a diabetes tracking system that has the ability to store up to 250 readings and associate each reading with an event label to help both the patient and the physician analyze the blood glucose level changes. The patient is able to link the Insulin dosage and type to each reading. The One Touch Profile has a data port that connects with a serial port of the computer to establish communications.

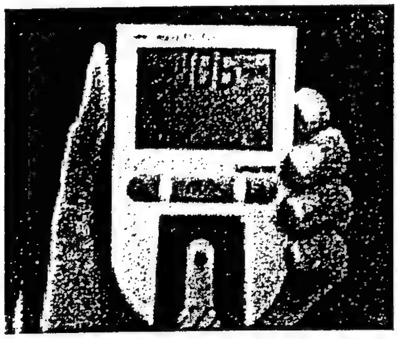
Each patient has a personal computer running Windows 95 and a 33.6-Kb modem. Data is transferred to the physician's computer via a standard telephone line.
The user interface between the One Touch meter and the database is "in Touch" Software which consists of two parts:

1. Diabetes Management: The patient will be able to transfer blood glucose readings stored in the Meter to the Diabetes Management Program, analyze current and past data stored in the "in Touch" database, and print reports that describe it. This program allow patients to set targets (high and low glucose levels), to see an average glucose level for a specified time frame, and to perform different file controls such as saving data, importing/ exporting, or archiving/restoring data. It also allows the patient to analyze meter settings, retrieve, view, and reset the meter's option settings, and delete readings stored in the meter's
2. Education: The diabetic patient or a member of his/her family will gain knowledge about diabetes and how to manage it by self-monitoring, controlling sugar level, eating a healthy diet, and exercising. Also, the program contains a variety of educational information on how to avoid the disease, and answer frequently asked questions.

Operational Protocol

For this preliminary study we randomly selected 10 patients with type I diabetes (Insulin dependents). They are being treated at Georgetown University Medical Center, and all are from the Washington DC metropolitan area. Their age varies from 13 to 65 years old. Each patient owns and uses a One-touch profile meter. It is a small device (approximately 4.5"x2.6"x1") that can be carried anywhere.

The patient is supposed to test his/her blood three times a day. The meter's memory automatically stores 250 readings.



One Touch Glucose Meter

Once a week the patient connects the meter's data port to the serial port of the computer. Then, the patient turns on both the meter and the computer. After the computer and meter is turned on, the patient runs the "in Touch" Diabetes management software and with one click all the readings are downloaded to the computer. The software reminds the user when a connection exists between the meter and the computer. Also, the software notifies the patient when communication is established. Once the data is downloaded the user is informed of the total number of readings in the database and the number of the new readings. The new readings are added to the existing ones each time the data is read.

The patient is able to list the meter readings by selecting the Data List report option. It is a raw report that shows the readings in a format very similar to the outline in which they were retrieved from the meter. At the bottom of the data list report, there is a window to associate comments with each reading. The patient has to select the reading he or she wants to add any comments to, and type the corresponding comments that could have affected the blood glucose at that time. Items that could have affected the blood glucose level include such things as food, exercise, and stress. If there are any other activities which the patient believes had an impact on his or her blood glucose level, he/she may wants to share the information with his /her physician. At this point the patient has to archive (store) the data to the computer's hard drive. We instructed the patients to use their names as filenames to be archived. The purpose was to avoid using different file names and getting the patient confused.

The program also offers more features and information to the patient and the physician such as:

- The Logbook Report. This report displays blood glucose readings and insulin dosages. Each entry summarizes one day.
- The Daily Details Screen. The screen shows more detailed data about a single day. It also lets the patient edit the data.
- The Data Statistics Report. It displays figures on blood glucose levels throughout the day, computed from all readings in the date range.
- The Average Readings Report. Charts are displayed. These charts illustrate blood glucose levels throughout the day and week, computed from all readings in the date range.
- The Readings within Target Report. This report presents statistical charts of within-target and out-of-target readings computed from all readings in the date range. The report uses the overall target range to determine which readings are within target in all time slots. Blood glucose levels above 600 mg/dL (33.3 mmol/L) are treated as if they were equal to 601 mg/dL (33.4 mmol/L), no matter how high they actually were.
- The 14-Day Summary Report. Tables and charts are displayed. They summarize blood glucose levels and related information over a period of up to 14 days, ending at the end of the reporting date range.
- The Glucose and Insulin Graph Report. Both graphs cover a period of 14 days. This report presents two graphs: one of blood glucose readings and one of insulin use.
- The Histogram Report. A histogram is presented. Each bar's height shows the number of readings that fall in a specified range of blood glucose levels.

Our goal in designing the system was to minimize the patient's input in the procedure of transferring data to the physician's side. After testing many possibilities, the patient's and the physician's input in the data transfer part was eliminated. A fully automated dial-up procedure was implemented to transfer the data from the patient's side to the physician's side.

A Macro was designed to run at a scheduled time each week. It automatically initiates the dial-up and performs the connection to the physician's office where a unique account was created for each patient. Also, the database is updated.

To retrieve a patient's data the physician runs the "in Touch Software", chooses a patient from the list, and restores his/her data. This allows the physician to view the latest data downloaded and identify patterns of glucose levels, select a specific reading and view the associated comment, if one exists.

The physician gives his feedback to the patient after reviewing the data. Then, the physician makes changes in insulin doses, exercises, or diet in order to optimize blood glucose level. Also, the physician can answer any concerns or comments the patients may have sent him along with their readings.

Findings

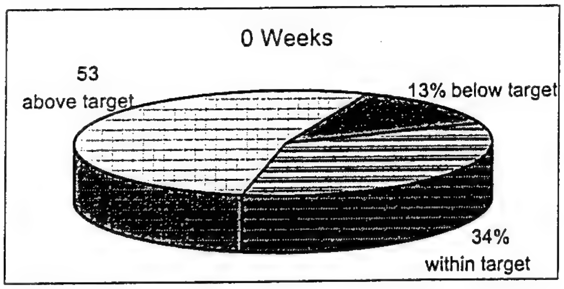
Patients showed a great interest in getting enrolled in the program. The patients enrolled who never used a glucose meter to monitor their blood sugar level found the program very motivating. They began to get their blood glucose readings on a regular basis.

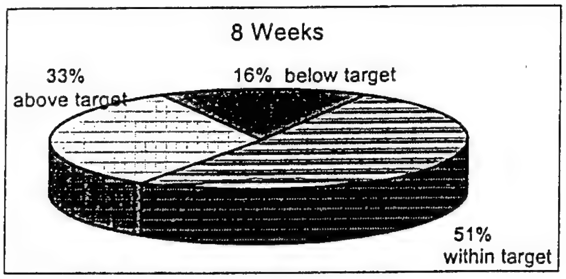
Hemoglobin levels, frequency of hypoglycemia, emergency room visits and hospitalizations measure glucose control. Preliminary data received by the physician automatically shows that the average number of readings per patient per day increased from 1.6 to 2.5.

The physician contacted patients and made suggestions to optimize blood glucose levels after analyzing data and looking into all patterns.

Patients who were not monitoring their blood glucose level prior to their enrollment begin to monitor their blood glucose level on a regular basis. Data shows a big improvement. Also the physician was able to bring within range blood glucose levels by changing insulin dosage, diet, and exercise.

The pie- charts below show the percentage of patients' blood glucose levels (within range and out of the recommended range) that were taken before and after enrollment in the study:





These pie charts show that after getting enrolled in the program for 8 weeks the average patients' glucose readings within range increased from 34% to 51%.

During this study none of the enrolled patients has had hypoglycemia or emergency room visit.

Discussion

Diabetes is a chronic disease that affects more than 16 million Americans and is characterized by serious, costly, and potentially fatal complications. Untreated diabetes can lead to many preventable diseases such as blindness, amputation, heart disease, and kidney disease. Fifthteen percent of U.S. health care dollars are spent on diabetes, $100 billion in direct costs (more than any other disease) and $140 billion with indirect costs.

Annually, 12,000-24,000 people with diabetes go blind. Diabetes is the leading cause of blindness, impacting 25% of patients. Annually, 54,000 people with diabetes require an amputation due to nerve damage. Twenty-forty percent of all patients' experience nerve disease. Annually, 20,000 people develop kidney disease requiring daily dialysis or transplant. Diabetes leads to kidney disease within 15 years of disease onset in 34% of all cases. The risk of heart disease and stroke is 2-4 times higher for people with diabetes. Sixty-five percent of people with diabetes also have high blood pressure.

A ten-year trial study sponsored by the National Institutes of Diabetes and Digestive and Kidney Diseases included 1,400 people with insulin dependent diabetes. This study showed that the patients in the "tight diabetes" <control> group lowered blindness cases by 76%, kidney failure cases by 56%, and amputations due to nerve damage by 61%. These patients kept their blood sugar levels close to normal by frequent blood sugar testing and changing their lifestyle such as exercising regularly and eating healthier.

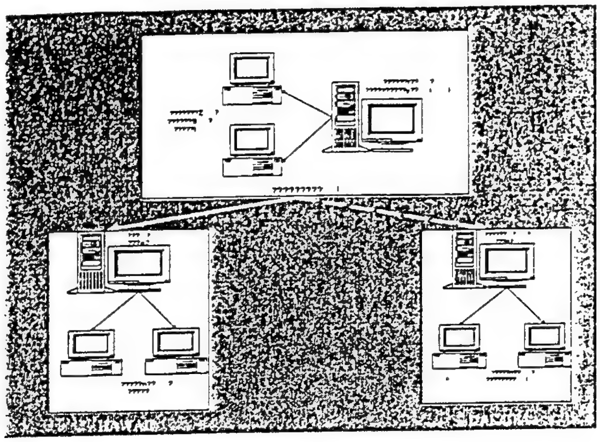
Conclusion

Treating diabetes early can improve health outcomes for diabetic patients. Therefore, routine screening and correct diagnoses are essential.

This is a cost-effective solution to bring health home to patients. As we mentioned earlier in this paper the requirements are basic. Today, a big majority of citizens can afford a phone line, a personal computer estimated at $ 500 or less, and a glucose meter estimated at $ 75. Diabetes telemonitoring offers the possibility of eliminating distance and time as a barrier to good blood glucose management, and a significant cost reduction in the short and long term hospitalizations, treatment and ER visits. It also offers disease prevention and a better quality of life.

Future Expansion

In a joint effort with Hawaii University and S. Dakota University similar projects are being implemented creating a network for monitoring diabetes patients.
The Physician at Georgetown University Medical Center will act as a consultant for these remote locations and communicate via email his opinions on consultations.



For more information
visit:www.telemedicine.georgetown.edu
www.rainbow.net/telemedicine

HIPAA Data Security: guidelines for organizational development in health information assurance

Jeff Collmann, Ph.D.,
Georgetown University Medical Center and
The Telemedicine and Advanced Technology Research Center
Ted Cooper, M.D.
Kaiser Permanente Northern California
Kristen Sostrom,
Tricare Management Activity, Office of the Secretary of Defense/Health Affairs

In

Bruce Reiner and Elliott Siegel, eds, *The Electronic Archive, SCAR Primer 2,* Society for Computer Applications in Radiology, in press

I. Introduction: Promoting a culture of information assurance in healthcare

Complying with the data security regulations of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 offers the opportunity for American healthcare organizations to develop cultures of health information assurance that add business value. This will require work on health information security at three, interrelated levels of organizational life, namely activities designed to implement plans for assuring health information security, organizational functions supporting health information security and organizational conditions that sustain health information security. . By activities, we mean all those tasks and programs that organizations accomplish in the name of improving the security of health information such as assessing risk, auditing logbooks, , and investigating security incidents. The proposed HIPAA data security rules identify most such pertinent activities. Organizations frequently sponsor activities while discharging broad functions that support health information security. Three functions seem particularly important, namely monitoring changing regulations, laws and professional standards; regularly reviewing, revising and enforcing data security policies, procedures and practices; and enhancing patient and business associate understanding of an organization's data security program. *The CPRI Toolkit: managing information security in healthcare* offers guidance on establishing these functions in healthcare organizations[1]. Sustaining such security-related activities and functions, however, requires organizations to bridge social boundaries that tend to reduce communication and collaboration about data security among their constituent disciplines and units thus isolating health care information assurance from its use. Organizations bridge boundaries by sponsoring interdisciplinary, interdepartmental work groups, establishing formal partnerships among people and units responsible for all aspects of information management, and encouraging communities of proponents who support sound health information security practices across the enterprise. As healthcare organizations extend clinical information systems outside the boundaries of their conventional business domains, assuring patients, collaborating physicians and business associates of the confidentiality, integrity and availability of information resources becomes a strategic requirement for continued growth.

II. HIPAA: guidelines for strategic development of health information assurance

Most observers expected the Department of Health and Human Services (DHHS) to release the final rules on data security required under the Health Insurance and Portability Act (HIPAA) of 1996 by January 1, 2001. The Clinton administration decided to focus attention on the proposed medical privacy rules thus releasing them on December 28, 2001 and postponing release of the final medical security rules. As of this writing in mid-winter 2001, DHHS expresses continuing uncertainty about the date of final data security regulations. In the face of such uncertainty, what actions should responsible healthcare organizations take with respect to the data security rules? Should we, too, delay or, perhaps, ignore the rules? Or, could we use the proposed security rules as guidelines to good practice in developing a long-range plan for protecting our clinical information systems? We adopt the position that because the proposed data security rules manifest good computer and information security practice, they represent guidelines for strategic development of a healthcare organization's general health information assurance effort. Hence, healthcare organizations can responsibly plan using the draft rules without fear of taking actions potentially undermining compliance. We argue, furthermore, that the HIPAA compliance effort can become an opportunity to manage change that will modify the culture of the organization to deliver business value and support multiple compliance efforts.

The final HIPAA data security rules remain under government review as of mid-winter 2001 with varying estimates of their release date Even though some details of the final rules will differ from the Notice of Proposed Rule Making (NPRM), the proposed HIPAA data security regulations constitute guidelines for strategic development of health information assurance. DHHS intentionally drafted the rules as parameters of planning rather than definitive steps. The proposed rules also heavily emphasize sharpening administrative management of data security and leave broad discretion for technological implementations. Assessing and managing information security risk constitutes the heart of the HIPAA data security proposals thus both mandating and encouraging healthcare organizations to exercise judgement in developing their compliance efforts. Because focusing on the administrative provision is the key to achieving compliance, healthcare organizations may use the proposed rules to help plan their health information assurance programs with confidence of achieving ultimate compliance

Who must comply? All health plans, clearinghouses, and those healthcare providers that use any of the standard electronic transactions ("covered entities") must comply with HIPAA. Some comments on the draft rules noted confusion about when health care providers become "covered entities" and, thus, subject to the rules. The draft rules leave unclear whether all providers who use electronic media or only providers engaged in covered electronic transactions qualify as "covered entities". Authoritative sources indicate that the rules do not require health care providers to comply who maintain or transmit health information in electronic form but have not yet made electronic transmissions in connection with a standard transaction. Once they make an electronic transmission in connection with a standard transaction, they must forever after comply with the data security rules. The rules apply to any and all electronic transactions of protected health information and remains applicable even if the provider never makes any more standard transactions in electronic format.

What strategic guidance do the draft rules provide? The requirements or standards are divided into four categories: administrative controls, physical safeguards, technical security services, and technical security mechanisms. Each category includes two types of rule, mandatory requirements and addressable implementation features. A covered entity must implement all mandatory requirements. Covered entities must also assess each addressable implementation feature in light of an information security risk assessment (see below for details of risk assessment). If the results of the information security risk assessment highlight a problem with a particular addressable feature, the covered entity must take action to mitigate the risk. Grouping mandatory requirements and addressable implementation features under a major rule elucidates the rule's intent and how it should be met. Designating implementation features as "addressable" allows the standard to be scalable. What is appropriate for one entity may not be appropriate for another based on variables such as size, differences in system architecture, and operational environment. Occasionally, a requirement appears to be repeated. For example requirements for access control are found under Administrative Controls, Physical Safeguards, Technical Mechanisms and Technical Security Services. Each of these requirements addresses a different aspect of access control depending on the category in which it is found. Although the repetitions appear to be redundant, they actually stress different aspects of assuring satisfactory control of access to protected health information. As with JCAHO and other health compliance activities, HIPAA requires good documentation on the reasons for the decisions made, particularly of decisions not to implement an addressable feature.

Administrative Controls

The HIPAA data security NPRM focuses attention on developing strong administrative controls for protecting the confidentiality, integrity and availability of protected health information. The majority of all mandatory requirements and addressable features fall under this category. Using the draft rules from this category to begin planning a health information security program will significantly prepare a healthcare organization to comply with the final data security rules once released, improve its health information assurance overall, and provide business value. Several administrative controls occupy truly strategic positions in a healthcare organization's information protection strategy.

"Security management process": All covered entities must establish a "security management process" that creates, administers, and oversees policies to ensure the prevention, detection, containment and correction of security breaches. This requirement mandates a "life cycle approach" to security; that is to say, an organization must assess its security posture and work to reduce its risks on a continual basis as the security environment and needs of the organization change. To meet this requirement a covered entity must assign responsibility for information security throughout the organization and engage all levels of management in the compliance process. To emphasize the importance of this requirement all of the security management process requirements are mandatory, namely risk analysis, risk management, sanction policy, and security policy.

Risk management constitutes the heart of complying with the HIPAA data security rules. Each covered entity must conduct a risk analysis that includes assessments of its information assets, threats to those assets, its own vulnerabilities to threats, and the impact of breaches on its operations. The risk analysis should include organizational and technical assessments that address all areas of information management (including health care delivery and administration, not only the technical information systems. After completing its risk assessment, a covered entity must develop actions, plans, and strategies to protect itself from breaches of the confidentiality, integrity and availability of its information assets. When selecting protective measures, covered entities should include cost effectiveness as a criterion. Because HIPAA compliance depends upon risk assessment, covered entities may legitimately select different solutions to similar problems depending upon individual circumstances. No single approach to HIPAA compliance exists or meets the needs of all covered entities. Covered entities should continually use the results of periodic risk analyses to maintain and improve their security posture as circumstances require.

HIPAA requires covered entities explicitly to state the objectives of their security management program in a formally documented organization security policy. The policy must assign responsibility for developing, implementing and enforcing the covered entity's policies, procedures and practices. Developing methods to recognize, report and respond to "Security Incidents" constitutes an important administrative support for policy implementation. HIPAA also requires covered entities explicitly to communicate to each and every employee, agent, and contractor the disciplinary actions to be taken in case of a breach, including verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment, contract penalties and notification to law enforcement officials and regulatory, accreditation, and licensure organizations. Such communications must explain the civil or criminal penalties for misuse or misappropriation of health information

Five additional strategic "Administrative controls" augment the central role of the security management process in protecting a covered entity's information assets, namely personnel security, training, contracts with business partners and associates, contingency planning and certification.

"Personnel security": Personnel controls ensure that all personnel who have access to protected health information have the required authorities and all appropriate clearances. "All personnel" includes a covered entity's own employees, contractors, volunteers, students, trainees, all personnel with access to protected health information whether or not they directly provide patient care, and personnel who have access to hard copy output even if they lack access to the network. "All employees" also includes people such as equipment maintenance personnel who have physical access to the network but may not review the information. By "clearance" this rule means that, based on the results of its risk assessment, an organization should determine the type of screening process required for each job position or role and document the procedures to be followed in conducting that check. In the routine course of personnel management, covered entities should also closely supervise all personnel as they use information assets, document their access to protected information, instruct personnel in information security policies, procedures and practices, and require personnel to undergo formal termination procedures when changing jobs or leaving the organization.

"Training and awareness" campaigns constitute the basis for individual compliance with an organization's information security program. In addition to formal orientation, annual updates and topical security reminders, HIPAA encourages covered entities to sponsor ongoing activities that heighten all personnel's consciousness about the importance of sound security practices. In order to assess the impact of such activities, covered entities must document what their personnel understand as well as their own efforts. Training and awareness campaigns represent an example of a HIPAA rule codifying practices all healthcare organizations should already be sponsoring.

"Controlling business partners": In both medical privacy and data security, HIPAA seeks to strengthen controls covered entities exert over their business associates in the exchange of protected health information. Given the contentiousness of this provision, its details might be expected to change in the final rules. The issue resolves fundamentally to another question of risk management: how much responsibility and liability does a healthcare organization want to take for its business partners' shortcomings in protecting health information? Whatever the final requirement, healthcare organizations must develop an approach to this question.

"Contingency planning" often gets short shrift in healthcare. Widely recognized as a necessary business practice, other priorities often take precedence over disaster recovery and business continuity planning. The HIPAA data security rules will change this situation by requiring all covered entities to implement the key dimensions of sound contingency planning in information management, including applications and data criticality analysis, data backup plan, emergency mode operation plan, and testing the contingency plan. Testing serves two well-known purposes, namely, training for those who must carryout a contingency plan and assurance that the plan is appropriate and will work. Failures in the testing process provide a means for correcting and improving the plan thus providing something that works in a real emergency. Close examination of fully developed contingency planning policies such as US Army AR25 IA PAM documents the fundamental importance of this process for a comprehensive approach to information security: healthcare organizations should plan for when breaches happen, not whether breaches happen. Covered entities will have to "certify" that their efforts to mitigate data security risks have implemented the standards established during their own risk assessment. This requirement emphasizes the "life-cycle" approach to risk management outlined as part of the security management process regulation and thereby brings risk management full circle. Good risk management plans become incorporated into everyday practice and do not disappear into an administrative drawer once signed. By documenting that they are providing the level of protection promised at the beginning of the process, covered entities demonstrate their compliance with this fundamental strategic goal of health information assurance.

Physical safeguards

The mandatory requirements and implementation features under the "Physical Safeguards" category focus special attention on protecting access to and the integrity of the physical artifacts of a health information system from all human and natural threats, including but not limited to intrusion, flood and fire. A good physical security plan will include policies, procedures and practices that always and only provide authorized, necessary access to health information assets during routine and emergency operations. Covered entities must document who gains access to and modifications of their information assets, including visitors. HIPAA focuses special attention on the movement and use of all information media, particularly workstations. Covered entities must specify who has access to which workstations for what purposes in all instances.

Technical Security Mechanisms and Services

HIPAA requires covered entities to evaluate technical controls for protecting data at rest and in transit. These technical safeguards differ from administrative controls because they constitute or function as part of an automated information system rather than as actions executed by people. HIPAA's approach to the general problem of information access control illustrates the difference between administrative and technical controls. Under the administrative category, HIPAA requires developing policies and procedures that establish different levels of access by role or individual to health care information, including procedures for establishing, modifying and authorizing initial access to information resources. Under technical security mechanisms and services, HIPAA requires technical means to enforce information access policies, including unique user identification codes, emergency access and "entity authentication" referring to machines as well as individuals. In order to promote monitoring of system access, HIPAA requires auditing of system activities. In addition to controlling access, HIPAA also seeks to protect the confidentiality and integrity of health information through encryption and data authentication techniques, particularly for data in transit over open public lines such as the Internet.

III. HIPAA: an opportunity for organizational development and business value

Healthcare organizations may find assistance in developing a health information security program from *The CPRI Toolkit: Managing Information Security in Health Care,* a publication of the Computer-based Patient Record [2]. Recognizing the importance of information security in managing computer-based patient records, the Computer-based Patient Record Institute (CPRI) chartered the Work Group on Confidentiality, Privacy, and Security to promote this process. Since its inauguration in 1993, the Work Group has developed and published a series of topical guidelines on improving information security for organizations implementing computer-based patient record systems. The guideline series addressed individual issues in information security, but, taken as a whole, promotes a comprehensive organizational process. The CPRI believes that managing health care information requires integrating good security processes into the everyday working routines of all staff, not just implementing security measures. Toward that end, the CPRI charged the Work Group to consolidate its guideline series into a toolkit that outlines general principles and provides "best practice" examples of how health care providers should manage the security of their paper and electronic records. Each section of the *CPRI Toolkit* includes an introduction, a copy of the latest edition of the pertinent CPRI guideline, several case studies with sample policies, procedures and forms, and extensive references to print and Internet sources of more information. A consolidated annotated bibliography, a list of Web sites, and a glossary of terms appear at the end of the CPRI

Toolkit. With this toolkit, any healthcare provider should be able to plan, implement, and evaluate a security surveillance process scaled to their organizational needs. Originally published in April 1998, the third edition of the *CPRI Toolkit* was released in April 2000 with subsequent editions planned as revisions become available. It may be obtained on the web at http://www.cpri-host.org or in hard copy from CPRI-Host, Bethesda, Maryland.

The organization of the *CPRI Toolkit* addresses each of the three critical security functions: monitoring their federal, state and professional regulatory and legal environment, updating their own internal environment of policies, procedures and practices, and communicating with their patients. As healthcare organizations work their way through the critical steps of the security surveillance process, they will find resources in the *CPRI Toolkit* linking the process to these three broad functions.

1) Monitoring Laws, Regulations and Standards: Chapter 3 devotes great attention to the extensive HIPAA-provoked federal activity in health information security and provides extensive materials about state and professional activities in health information assurance. This chapter includes summaries of all the HIPAA electronic transaction, data security regulations and medical privacy. A section on state law includes information on how to investigate legislative action in all fifty states as well as a recent evaluation of the state scene prepared by the Georgetown University Health Privacy Project. The Executive Summary of the JCAHO/NCQA Recommendations for Protecting Personal Health Information is republished with permission in recognition of the central role of these two accrediting bodies for healthcare providers. The third edition includes a discussion of the implications of the European Directive on Privacy for American organizations managing personal information of European citizens. Finally,

DHHS and professional information security specialists regularly refer to and depend upon the work of a range of standards setting organizations, a realm that often remains somewhat obscure to many healthcare professionals. In order to demystify and recognize the importance of standards setting organizations, the editors of *CPRI Toolkit* asked Margaret Amatayakul, former executive director of the CPRI, to write an introduction to setting standards in health care information. Using the resources in this section of the *CPRI Toolkit*, any healthcare organization ought to be able to discover and track the various federal, state, and professional requirements in health information security and privacy to which they must comply. HIPAA gives this section special salience now; but, monitoring laws, regulations and standards for healthcare constitutes work that never ends for healthcare organizations in this and all aspects of their operation.

2) Updating health information policies, procedures and practices: Since its inception in 1993, the CPRI Work Group on Confidentiality, Privacy and Security has published booklets on specific topics in health information security. Each booklet is reprinted in Chapter 4 accompanied by samples and case studies illustrating the critical steps healthcare organizations should take to plan and implement a health information security program. Sample security policies illustrate how eight different healthcare organizations of varying scale have addressed the issues discussed in "CPRI Guidelines for Information Security Policies." To learn about "Assigning Roles and Responsibilities" in health information security, consult the reprinted "CPRI Guidelines for Managing Information Security Programs" and a case study from the University of Pennsylvania. An authoritative introduction to information security risk assessment and a case study risk assessment of a telemedicine project in hemodialysis provide valuable aid

to starting this central process. A comprehensive information security training course complete with "Instructor's Guide", all necessary slides, and pre and posttests accompanies the "CPRI Guide to Information Security Training". Information about organizations that sponsor regular training in information security training and references to other resources complete the section. To learn about how organizations enforce security policies, consult the sample confidentiality statements/agreements and a case study on securing user agreement at Kaiser Permanente Northern California. A special section focuses on issues in the electronic transmission of health information such as email, fax and the Internet. HCFA's new Internet Policy appears accompanied by a discussion of PCASSO, an NLM-sponsored project giving patients and providers secure remote access to computer-based patient records at the University of California San Diego Medical Center. This includes discussion of certain information security technologies such as firewalls and encryption. The third edition includes a discussion of the Connecticut State Hospital Associations state-wide Public Key Infrastructure (PKI) project, a useful introduction to a vital technology.

3) Enhancing patient understanding of an organization's health information security program. In the new millennium, patients will hold healthcare organizations accountable for many aspects of their business practice as well as medical care. Congress continues to debate Patients' Bill of Right legislation to permit suit of managed care companies for denial of service and other business practices. Such bills and supporting anecdotes provide some evidence of public dissatisfaction with the consequences of reforms in healthcare finance during the last decade. Demands for greater accountability in the use of personally identifiable health information reflect distrust of complex

organizations and their power over the lives of individuals. The recently released final medical privacy regulations require healthcare organizations to permit patients to review and propose corrections to their medical record as well as document and permit patients to review lists of disclosures, other than those for treatment, payment or healthcare operations. Chapter 5 of the *CPRI Toolkit* includes procedures and forms from AHIMA illustrating how healthcare organizations might responsibly provide these services. The final privacy rules also require healthcare organizations to post detailed, written explanations of their privacy policies and practices. Healthcare providers might actually go one step beyond complying with these rules and use the public's concern about medical security and privacy to build trust. Chapter 5, therefore, also includes an example of a patient-friendly, online introduction to health information security. Healthcare organizations should consider deploying such tools for informing patients about their business practices, particularly privacy and data security, as well as about managing their health.

IV. Sustaining health information security

Developing a sound information assurance program requires balancing the conflicting demands of security's three major elements, confidentiality, integrity and availability. Healthcare organizations should, therefore, develop work processes and organizational structures that promote communication about and mutual responsibility for security among the many and various constituencies contending for influence over the medical record. Without attention to these processes, conflicts over appropriate policies and procedures will isolate information assurance from its use and, thereby, promote security and confidentiality of patient identifiable information on its LAN. ISIS decided to investigate installing a firewall to enhance protection of information on its LAN. After sustained discussion among its staff, ISIS issued a Request for Proposals, accepted bids, and eventually installed a firewall protecting its LAN. The RFP addressed important technical components in the ISIS Center's approach to managing data security. Ongoing risk analyses, risk management plans and data security policies supported the technical approach being sought in this RFP. The ISIS Center does not function as a repository for clinical information; but, must nonetheless protect the security and confidentiality of patient identifiable information used in pursuit of its research mission.

Technical Environment of the ISIS CenterThe ISIS Center originally operated its LAN in an open, unrestricted mode[3,4]. Because the ISIS LAN was connected to untrusted networks, we designated it as open. Moreover, it functioned in a relatively unrestricted mode because few access controls or authentication measures existed beyond those provided by individual computers on the LAN. Anyone with rights to work on ISIS projects could use the equipment and the network with minimal password control. Vendors, other university investigators and students with whom ISIS investigators collaborate enjoyed unencumbered remote and local access to the ISIS LAN. Individual investigators exercised the responsibility for data security policies with little or no effort to educate users in or enforce a center wide security policy. Investigators also determined what services to use in their research, including modem access, telnet, web access and other functions. This approach to data security met the needs of ISIS when research inconsistencies in practice that undermine an organization's ability to implement any concerted approach to health information assurance.

Case Study One: Securing the ISIS Center

The Imaging Science and Imaging Systems (ISIS) Center, Department of Radiology, Georgetown University, conducts research in applications of advanced computing and telecommunications technology to health care. In its capacity as an important civilian research laboratory for the Department of Defense, the ISIS Center has established its reputation for technical sophistication and organizational effectiveness through projects such as DINS (the prototype and technical specifications for the DOD filmless radiology system known as MDIS), Project DEPRAD (the deployable teleradiology network built in support of NATO troops in Bosnia), and digital mammography (proof of concept and working model of digital mammography adapting computed radiography technology). The ISIS Center also successfully competes for extramural funding from other government agencies including the National Institutes of Health and the National Science Foundation in the areas of image processing, computer-aided diagnosis, telemedicine, and image guided therapy.The ISIS Center faces major changes in its research environment. On the one hand, projects in all aspects of its work are beginning to acquire, manipulate and archive patient identifiable information on the ISIS Center local area network. This includes running clinical trials for government and commercial funding agencies subject to Food and Drug Administration rules and regulations. On the other hand, investigators, physicians, and patients increasingly require remote access to such data using dial-up and web-based technology. Whereas the ISIS Center has historically not faced major data security problems in its links with untrusted networks, these two new conditions require developing a plan for managing the projects functioned without patient identifiable data and before we conducted clinical trials.

By installing a firewall, the ISIS Center changed its mode of LAN operation to an open, restricted mode. The ISIS LAN remains connected to untrusted networks, including the Internet. The firewall installed access control measures that enforces new policies protecting patient identifiable data and meeting data security requirements of our funding agencies. Individual investigators retain the right to determine access and use privileges for data in their own projects consistent with the data security policies of the ISIS Center and their funding organizations. Their policies are documented and included formally as appendices to the written ISIS Center data security policies, including lists of authorized users and their privileges. Each investigator collaborates with the ISIS Center network administrator in appropriately programming access and authentication tables in firewalls and databases to enforce policy. The ISIS Center also depends upon the professional ethics of individual staff as a constituent component of its security policy. This approach will attempt to incorporate the autonomy and responsibility of investigators conventionally associated with a research environment into practices increasingly expected of all organizations creating, manipulating and archiving computerized patient identifiable data. The decision-making environment of the ISIS Center

Because the new data security policies and procedures affected the work of independent investigators and highly sophisticated staff who previously enjoyed wide autonomy in their use of services, all ISIS staff collaborated in designing the new system. Over a period of several months, ISIS staff convened meetings to discuss key issues related to the firewall, including the individual and collective need to communicate with networks outside of the ISIS LAN and potential architectures of the ISIS LAN after installation of the firewall. Although most of the staff are technically trained and experienced in advanced computing and telecommunications technology, few claimed any real expertise in "computer security". Above all few had direct knowledge or experience with firewalls or their impact upon system performance. These discussions were an initial opportunity to investigate the technology and implications of enhanced network security. Throughout the entire discussion, ISIS staff expressed great concern about potential declines in availability and network service as a result of installing the firewall, particularly reductions in network speed and the possibility of firewall failure. The debate about access to the outside world and the future architecture of the ISIS LAN fundamentally concerned negotiating the tradeoff between security and service the ISIS staff was willing to accept in light of its new responsibilities and mission. Although organizations can mandate such tradeoffs, ISIS tried to coopt not coerce its staff into making the decisions.Defining the LAN Architecture

The ISIS LAN connected directly to the Georgetown University network through a router located on the first floor of 2115 Wisconsin Avenue with two hubs in a communications closet across the hall from the ISIS Center which is located on the sixth floor of the building. No firewall previously controlled access to the ISIS LAN or to the 2115 segment of the Georgetown University LAN. The ISIS LAN network runs on 10BaseT Ethernet and ATM media using TCP/IP and IPX/SPX protocols. The ISIS LAN supports a range of equipment including desktop personal computers, high end workstations, Wolfcreek magnetic tape silo and the usual peripherals.

ISIS intended to enhance the security of the ISIS LAN, software and data by installing a firewall between some parts of the ISIS LAN and the Georgetown University network. Determining the number of firewall interfaces and thus domains of the ISIS LAN became a major issue in discussions. A firewall segments a network into trusted and untrusted domains by restricting access to some segments of the network. A segment becomes "trusted" because the firewall restricts access to only those users who have permission to enter according to the organization's security policy. Networks or network segments not subject to the organization's restricted access policies become "untrusted" by that very fact even if they function as part of its overall infrastructure. Please note: the concepts of "trusted" and "untrusted" are relative. A particular network segment may be "trusted" with respect to one network but "untrusted" with respect to another network. For example, people often think that firewalls guard internal networks from the Internet thus making the Internet an "untrusted" network and the internal network a "trusted" network. Many firewalls will support more than two interfaces, however, and thereby permit two or more network segments to be shielded from the Internet. Both network segments may be "trusted" with respect to the untrusted Internet; but, untrusted with respect to each other. Adding interfaces and increasing network domains increases security but adds burdens. The question for the ISIS staff was whether to create one or two trusted domains on the ISIS LAN. After much discussion ISIS decided that upon installation of the firewall, two ISIS domains should exist, an internal, trusted domain protected by the firewall and an external, untrusted domain not protected by a firewall.

The answers to several questions conditioned the final approach to the firewall, including:

1) Where will the patient identifiable data reside? In discussions of the firewall, ISIS reviewed use and storage of patient data. The ISIS LAN included a magnetic tape silo with the intent of modeling a centralized archive. ISIS decided nonetheless to plan as if data might be stored and/or used on almost all ISIS computers, including but not limited to the magnetic tape silo. This decision reflects two fundamental features of ISIS work; namely, that principle investigators manage projects, not the ISIS Center and data potentially moves throughout the ISIS LAN during use irrespective of where it may become archived. The infrastructure should support the principle investigators and protect patient identifiable data wherever it may temporarily or permanently reside.

2) How shall ISIS researchers access patient data? ISIS researchers previously gained access to and manipulated data from any point on the ISIS LAN including their desktops, home and other remote locations. On the one hand, everybody understood that some kind of restrictions on access from outside the ISIS Center were necessary. The question remained of how much control should be exerted on traffic on the ISIS LAN itself. This question depended in part on the answers to the question above because, as ISIS studied the issue, it realized that daily use does not clearly draw the line between investigators and other staff as well as the line between "workstation" and "archive". Potentially every person and every machine became responsible for patient identifiable information. Thus, traffic inside the trusted ISIS domain should flow unimpeded by the firewall.

3) How much effort did ISIS want to invest in maintaining interfaces? ISIS's lack of experience with firewalls raised concerns about the effort and expertise needed to maintain multiple interfaces. Purchasing expert support was possible and inevitably necessary. The fact remained that the ISIS staff would function on the frontline of the firewall war and did not want to mortgage the ISIS Center just to maintain the firewall. The ISIS staff adopted the KISS principle: until ISIS become more experienced and confident of its ability to manage problems with the firewall, it should minimize potential sources of trouble.

In light of all these conditions, ISIS selected the option of a single trusted domain and a single untrusted domain as illustrated above. Such an arrangement created a secure domain for managing confidential patient information while supporting the ISIS Center's investigator driven approach to managing research projects. ISIS could more easily maintain the firewall as it gained experience in its use and operation. Finally, ISIS decided to compensate for potential technical limitations of security by training ISIS staff and depending on their sense of professional responsibility

Communicating with the Outside World

Before installing the firewall, the ISIS staff routinely communicated with the outside world from the ISIS LAN and with the ISIS LAN from the outside world using a variety of protocols. In order to enhance security on the LAN, ISIS had to restrict access from outside to authorized personnel, but not sacrifice use of communication tools. This made a certain kind of firewall known as a proxy or application firewall necessary. Proxy firewalls "open" packets in specific applications such as FTP, Telnet, SMTP, and HTTP thus enabling exact identification of their source. The inspection process exacts a

When should the consultation end? ISIS tried to include the staff in all phases of the decision-making process including needs assessment, architecture definition, RFP preparation and bid evaluation. Almost every body participated in the needs assessment and architecture definition. Many staff commented on the RFP drafts but almost none on the bids. Perhaps evaluating the bids is perhaps on the other side of an invisible line of knowledge and responsibility the staff expects only the security team to cross. When the time came actually to choose the firewall, all ISIS staff nonetheless jumped back into the decision-making process.

How widely can consultation occur in large organizations? The ISIS Center has a staff of approximately thirty people that routinely supports collective projects. In spite of its potential impact on the ISIS Center, installing the firewall is a joint project like many others at the ISIS Center. The small scale and general operating philosophy supports cooptation. Making cooptation function in a large-scale organization requires careful planning and perhaps more formal approaches than ISIS found necessary. Kaiser Permanente's approach to the trustee-custodian relationship and to developing regional and national security teams offers good instruction on this issue (see Case Two below)

Finally, how does interdisciplinary consultation work in organizational settings more hierarchical than the ISIS Center, many academic research laboratories, or for that matter medical centers. Imposing infrastructure solutions on people may be routine in most "real world" organizations. Nonetheless, some element of cooptation, engaging people in making the unpleasant decisions that affect their lives, is necessary in the area of data security if we are to create security capable organizations. The question is how to accomplish this task outside the context of small, face-to-face settings like the ISIS

Center. Through the development of interdisciplinary medical information security readiness teams and a world-wide culture of proponents, the Department of Defense is using HIPAA to attempt to address this question in a global, multi-tiered organization (see Case Three below)

Case Study Two: Kaiser Permanente's Trustee/Custodian Agreement

In large organizations, the differentiation of work roles, particularly between clinical and non-clinical staff, threatens to isolate information security functions from information use. In an effort to overcome this problem, Kaiser Permanente has created two special roles, the information trustee and information custodian. The information trustee and custodian link regular staff and information technology and security specialists. By creating the trustee/custodian relationship and documenting it in a formal "Trustee-Custodian Agreement", Kaiser has institutionalized mutual responsibility for secure information control between clinical and information staff, thus integrating not segregating it from everyday workKaiser Permanente supports the daily work of the trustees and custodians with regional information security committees that integrate information security with other key issues such as data quality.

Data Trusteeship at Kaiser Permanente Northern California

In recent years, more essential business functions have become dependent on information technology; therefore, the way business systems are designed and implemented by Kaiser Permanente Northern California Region (KPNCR) has evolved. To keep up with the rapid changes brought on by technological growth, KPNCR must adapt and fine tune its approach to design and implement systems that provide security and promote higher data quality.

In January 1996, the Trustee Project was initiated in response to various audit recommendations and criteria of the National Committee for Quality Assurance. The project:

- Identifies and/or verifies Trustees for KPNCR's data processing resources (objects), regardless of platform (applications, operation files/databases, reporting/filing databases, transactions)
- Maintains information in a comprehensive, centralized list for KPNCR employees
- Establishes an infrastructure to implement a continuing process to grant access to these resources
- Follows the initiatives already implemented by Kaiser Permanente Southern California

This document provides guidelines on the roles and responsibilities of trustees and custodians in relation to data quality, usage, classification, and protection.

Roles and Responsibilities

The Trustee is an individual manager or agent of the manager accountable for leading, managing, and administering activities related to an application and its data. This is an individual responsible for the care delivery or health plan side of Kaiser Permanente rather than from information technology. The Trustee:

- Determines logical controls for KPNCR data assets
- Determines how a business application and its data are used and develops and communicates policies, standards, and procedures that are consistent with Regional policies, standards, and procedures

- Approves access to data by users
- Audits and monitors applications for appropriate access to and use of data
- Initiates corrective action in the event of inappropriate or unauthorized use
- Identifies data belonging to the application and classifies it according to "classification criteria"
- Defines control mechanisms for classified data
- Ensures that access audit reports are being monitored
- Specifies acceptable level of data quality during the development of an application
- Approves requests for changes to production data outside the normal business process
- Designates one or more surrogates to act on his or her behalf if necessary

The Custodian is the individual or organization entrusted with the physical possession or management of the system and data. All systems and data must be assigned to a Custodian. The Custodian may or may not belong to the Information Technology (IT) organization. The Custodian is responsible for:

- Implementing measures to ensure that the media upon which the data is stored are physically secure
- Ensuring that sensitivity levels are technically enforced
- Ensuring the availability of data for processing on a continuing basis
- Implementing technologies that secure data during transmission over private or public networks
- Implementing storage technologies under which processing is optimized

- Implementing storage and retention procedures
- Developing and implementing backup, recovery, and business resumption plans to ensure that the impact of any system failure or disruption is minimized
- Ensuring the availability of backup data

Data Issues

Data Issues can be classified as quality issues or security issues. This section focuses on the definition of both types of issues and their characteristics.

Quality Issues

Quality issues refer to data that is consistent with its expected value. The expected values should be defined by the Trustee at the time the application that collects and stores the data is developed. Implicit in this definition is that data are captured and maintained in the source applications and support the business activities of its users. Quality of data is the responsibility of the collecting application.

To ensure quality is high or that the expected value has been captured, data should possess the following characteristics:

- Accessibility: must be available to the client
- Integrity: processing of the data must not change the business meaning of the data
- Availability: current and available to the client when needed
- Accuracy: must represent correct values
- Consistency: consistently valued and can be shared across the business entities

Any inconsistencies that arise related to the characteristics should be addressed as quality issues. Types of quality issues are:

1. Inaccurate data: may be caused by errors in data entry, errors in transformation, or errors in querying the data. An example is the Diagnostic Related Group (DRG) table with fields that have shifted to the right one character causing the DRG 124 to become 12. This would result in the reporting of an entirely different DRG.
2. Incomplete data: may be caused by applications that do not consistently value pertinent fields within their system. An example is the provider field that identifies a member's primary care provider. This field only has value if a primary care provider has been designated. Incomplete data will exist for those members who do not have a primary care provider designated.
3. Inconsistent data: may be caused by applications that have been developed over time that report similar information with different formats. An example is the birth date. On the membership database, this field is six characters, but on the patient demographic database, the field is eight characters.
4. Missing data: results from operational applications that did not collect the required information for whatever reason. An example would be the ordering provider on the radiology application. If an area chooses not to collect these data, the field operationally defaults to the department chief.
5. Non-Captured data: results when data have not been captured for the input source. This issue relates to expectations of users. An assumption may be that members height and weight are captured in the Reg Plus application. This would be an inappropriate assumption given that this is an appointment registration system and is not designed to capture clinical information.

Security Issues

Security issues refer to:

- Data, image, and text security and application systems controls not in accordance with the ICPS policies, standards, and procedures
- Unauthorized attempts to gain access to data
- Unauthorized use of data (those not authorized by Trustee to access data)
- Any breach of information confidentiality

Data Classification

All corporate data, regardless of medium, is classified according to its value and level of sensitivity. Classification refers to a rank assigned to data based on the real monetary cost to replace the data and the degree to which disclosure or misuse could damage a patient, customer, business partner, or KPNCR. The classification/level of sensitivity determines the access controls to be placed upon the data.

Within general categories of data (e.g., patient medical record), some data may be considered more sensitive or critical than others. Inappropriate disclosure of some information in the patient medical record (e.g., mental health) , whether accidental or intentional, could be especially damaging to the patient. Therefore, this data shall have a higher level of classification. Kaiser Permanente uses four levels of data classification; public, internal, confidential, and registered confidential. There are different access, encryption, and auditing requirements for each. For more information, consult *The CPRI Toolkit.*

The Information Confidentiality, Privacy, and Security Group (ICPSG) represents major organizational groups within KPNCR irrespective of the organizational entity. This group is responsible for establishing, maintaining, and monitoring compliance with policies, standards, and procedures, as well as discussing and resolving issues related to information security. The ICPSG has published Regional policies, standards, and procedures regarding confidentiality and data classifications.

The Data Quality Leadership Team (DQLT) leads the effort to identify, organize, and integrate KPNCR's many systems currently in operation to ultimately improve the quality of data. This group allows KPNCR to make timely and appropriate clinical and business decisions. The DQLT is responsible for:

- Developing data quality policy
- Providing oversight of the implementation of the Data Quality Administration Plan
- Monitoring and evaluating data quality within KPNCR
- Improving the data quality administration process
- Reviewing and approving plans for data quality system issues that conflict with Regional data quality policies
- Establishing process teams after reviewing current data quality efforts and requirements

Conclusion

Not all healthcare providers require developing an arrangement as formal as Kaiser's Trustee/Custodian Agreement or comprehensive as regional security committees. Yet, most organizations larger than a single physician office differentiate between clinical and information systems staff. Formulating roles institutionalizing a sense of mutual responsibility for information security among staff operationalizes the idea that confidentiality is everybody's business. Instead of relegating information security to the technical specialists and parceling responsibility for managing patients only to clinicians, all staff assume responsibility for the enterprise, its patients, and the confidentiality of patient information.

Case Study Three: Preparing for HIPAA in the Department of Defense

Multiple conditions create boundaries inhibiting communication, collaboration and coordination about health information assurance (HIA) in the military healthcare system. Although federal laws, federal regulations and DoD provide guidance on HIA policies and procedures, the Air Force, Army, and Navy historically interpret that guidance in ways relevant to their own service traditions and operating conditions. The organization of health information assurance management reflects this relationship between the general and specific at the policy level with the Office of the Secretary of Defense/Health Affairs and the surgeons general respectively representing the DoD and service programs. For both the DoD and services, policies and procedures for information technology, medical records, and clinical care have developed relatively independently. From the perspective of IT policy, health care functions as just another application area with no officially recognized specific needs of its own. In spite of the ubiquity of the Comprehensive Health Care System (CHCS, the military's electronic patient record system) and multiple special applications such as MDIS (the military's computer-based radiology picture archiving system), medical records policy has only just begun to acknowledge the existence of computer-based healthcare records. The clinical, patient administrative and information technology chains-of-command similarly function with little formal regard for each other except at high level points of command. Military medical centers hospitals and ambulatory clinics (known by the acronym, MTF) constitute major points of organizational consolidation that exercise substantial responsibility and authority for many operational functions. With respect to HIA, each MTF must develop its own policies, procedures and practices again drawing guidance from higher directives but exercising discretion to adapt to local conditions. The MTFs represent the unit of compliance for many accreditation and regulatory processes such as JCAHO and HIPAA. In addition to all this complexity, the military health care system faces a variety of different contexts within which it must operate. The military health care system provides services across various "echelons of care" from medical centers in the United States to field clinics in deployment zones for members of the military forces, family members and civilians in both military and civilian treatment facilities. Moreover, information generated in one context often crosses boundaries through a variety of media to another context such as a wounded soldier who gets transferred from a battalion aid station in theater to a medical center well behind the lines. HIPAA implicates this entire spectrum of endeavor.

Bridging Organizational Boundaries

The Defense Health Information Assurance Program (DHIAP) is a Congressionally funded research project contracted to ATI, Inc. Charleston, South carolina under the oversight of the US Army Medical and Materiel Command, Telemedcine and Advanced Technology Research Center (TATRC), Ft. Detrick, Maryland. Two primary objectives of the, DHIAP will promote building bridges across these organizational boundaries in the military healthcare system, namely creating, training and equipping interdisciplinary Medical Information Security Readiness Teams (MISRT) at all MTFs and encouraging development of a Community of Proponents of

Health Information Assurance interweaving all levels of the military healthcare system. Achieving these two objectives together should incorporate health information assurance into the corporate culture of the military healthcare system thus supporting long term enhancement of medical information security readiness as well as achieving compliance with the HIPAA data security regulations.

Medical Information Security Readiness Teams (MISRT)

In letters sent to regional medical commands, MTF commanders and others, the surgeons general of the Air Force, Army and Navy directed appointment at all MTFs in the world of a HIPAA focal point and implementation team composed of three people representing the clinical, patient administrative and information technology fields. Developing the MISRT teams recognizes two important points: 1) medical commanders at MTFs bear ultimate responsibility for complying with the HIPAA data security regulations, and 2) the security of MTF information systems touches clinical and administrative work as well as the work of information technologists. Hence, representatives of all these fields should share responsibility for developing the MTF's approach to health information assurance.

The surgeons general also recommended that the teams attend training seminars on the content of and new tools for complying with the proposed HIPAA regulations being sponsored by TATRCand the Chief Information Officers of the Military Healthcare System. A discussion of the seminar agenda follows below. Please note two important points about the process. First, in order to build and create support for the MISRT, TATRC organized the training seminars on a regional basis. MISRT from all Air Force, Army and Navy MTF in each region attended a seminar together in a single location within their own region. For example, all MISRT in Region 1 including MTFs from Maryland, Delaware, Pennsylvania, New Jersey, New York, and all the states of New England attended a seminar in Bethesda, Maryland on January 26, 2001. Two, during the seminars, the MISRT worked together in breakout sessions. By jointly conducting exercises in policy review and risk assessment, the attendees get to know the members of their own MISRT and members of MISRT from other MTF. These exercises thus stimulate emergence of a regional community of practice with members from all MTFs, each military service (Air Force, Army and Navy) and each discipline (clinical, administrative, and IT). The DHIAP will continue supporting the local MISRT and regional communities of practice with follow-up training and a web-enabled, knowledge management portal named "RIMR" (see description below). The MISRT and the regional communities of practice should mitigate a primary threat to health information assurance: relegation of responsibility for information security to IT staffers operating in isolation from other staff at their own and other MTFs.

The training seminars also introduced MISRT to new policy analysis and risk management tools developed under the auspices of the DHIAP research effort. DHIAP sponsors an interservice, interdisciplinary Policy, Procedure and Practices (P3) Workgroup to compare all relevant Department of Defense and individual service regulations with the HIPAA data security regulations[5.] As part of this process, the P3 Workgroup developed various templates, matrices and report forms to conduct, document and analyze the results of the HIPPA-DoD policy comparison. The MISRT will similarly have to assess their own MTF policies as part of their HIPAA compliance efforts. During the seminar, Ms. Sostrom instructs the MISRT in the HIPAA regulations and introduces them to the P3 tools. The MISRT practice using the tools by reviewing and revising their MTF information access policies during the first breakout session.

During the afternoon session, the MISRT learn about two key tools being developed and implemented by the DHIAP, a web-enabled Risk Information Management Resource (RIMR) and a self-directed information risk assessment tool called "OCTAVE"[6, 7] OCTAVE enables the MISRT to discharge the central activity required by HIPAA, develop a health information security risk management plan[1]. As MISRTs begin implementing their risk management plans, they will require a variety of types of information about information security, including policy documents, risk databases, and technology reports. Using advanced computerized knowledge management tools, RIMR will consolidate and make such resources available to MISRT via the world wide web. OCTAVE is available on RIMR and eventually will link to RIMR risk assessment databases through a direct entry graphical user interface. EASEL, an information security simulation language also being developed under DHIAP, will also reside on RIMR. With respect to supporting the regional communities of practice, RIMR includes tools for creating regional and national webboards through which MISRT can query each other about security issues and share their experiences.

Community of Proponents for Health Information Assurance

Creating, training and equipping MISRT establishes new formal structures at the MTF level for managing health information assurance. The TATRC has also worked to develop informal new relationships that interweave formal DoD and service chains-of-command, agencies and operational levels in support of health information assurance. Given the relatively amorphous but nonetheless real impact of these informal relationships, we designate this emerging support network a Community of Proponents for Health Information Assurance. Like the Internet itself, the Community of Proponents will never exist as a defined structure with formal roles or boundaries. No Program Executive Officer will call a meeting of the Community of Proponents to take action on a security breach. Rather, the Community of Proponents addresses problems such as the lack of command support for information assurance. According to the GAO, commanders at all levels remain relatively indifferent to threats and vulnerabilities in the US defense computer network[8, 9.] Although one should focus attention on commanders themselves with new policies, increased indoctrination, and perhaps disciplinary action, such measures would fail to address the organizational conditions under which any member of the military practices or ignores sound information security discipline in their everyday work. Broad agreement, high expectations and routine good practice of health information assurance must exist woven into the structure of informal relationships that authoritatively govern and execute the chores of daily life. A discussion of efforts to disseminate information and build support for the DHIAP will illustrate these points.

Three lines of work have helped build support for the DHIAP, including executing an ongoing series of briefings about the project, sponsoring a triservice, interdisciplinary policy review called the Policy, Procedure and Practice (or, P3) Workgroup and participating in formal committees of the Office of Health Affairs. Because of the imminent need to comply with HIPAA and the range of health information assurance issues faced by the military health system, many agencies have an interest in the DHIAP. Since July 1999, TATRC has consequently responded to requests for and, in some cases, initiated briefings about the aims and ongoing accomplishments of the project. TATRC initiated this line of work by inviting representatives of critical agencies in the DoD and US Army information assurance effort to a strategic planning meeting in July 1999. Representatives from Office of the Secretary of Defense/Health Affairs (OSD/HA), the US Army Surgeon General, US Army Theater Information Management Program Office (TIMPO), the Information Assurance Technical Assistance Center (IATAC) and TATRC participated. This meeting produced agreement on key strategic thrusts for DHIAP, including development of a self-directed risk assessment tool (what became OCTAVE), a medical information assurance simulation tool, a method and examples of technical business case analyses for information assurance technology, a policy review initiative, a web-enabled knowledge management tool to make these tools available (RIMR) and a major educational effort to help MTFs enhance health information practice and prepare for HIPAA. The meeting also decided that the DHIAP's work should be expanded beyond its originally base in the Army to include the DoD, the Air Force and the Navy. A single theme underlies these strategic thrusts, namely maximizing the ability of MTFs to manage health information assurance at the local level.

TATRC consolidated these decisions into a strategic research plan, initiated the work and began briefing proponents in DHIAP's development, including, the Chief Information Officer and Designated Accreditation Agency, Office of the Secretary of Defense/Health Affairs (OSD/HA), the Chief Information Officers of each medical service, and others. TATRC continues refining and adapting the strategic research plan in response to emerging DoD and service health information assurance needs as this process unfolds.

The July 1999 meeting recommended initiating a review of DoD and service level policy on all aspects of health information assurance in light of the proposed HIPAA data security regulations. HIPAA posed a challenge to standard DoD practice in policy development for information assurance. HIPAA takes an integrated approach to data security requiring coordination of administrative and technical work. From a policy perspective that means cross-referencing policies in medical records management and computer security. HIPAA also offered an opportunity for interservice collaboration in policy development. With these ideas in mind, DHIAP developed the Policy, Procedure and Practice (P3) Workgroup. The initial meeting included the chief medical records officers from the Air Force, Army and Navy Surgeons General offices, a representative of OSD/HA and TATRC. After conducting a preliminary analysis of medical records policies, the group decided also to seek representation of the information technology communities of each service. Thus the P3 Workgroup became an interdisciplinary and interservice activity.

The P3 Workgroup adopted a work process designed to take maximum advantage of its interdisciplinary, interservice composition. After working as a committee of the whole to develop and learn a joint approach to policy review, the P3 Workgroup split into two subgroups to work more quickly. One group included all representatives of the Navy and OSD/HA. The other group included the Army and Air Force representatives. TATRC representatives participated in both groups. These groups conducted exhaustive primary comparisons between the HIPAA data security rules and all pertinent policies of their respective services. After completing this primary review, each subgroup conducted a quality assurance review of the work of their counterparts in the other subgroup[10].

While this core dialogue and work produced an analysis of policies, it simultaneously linked distinct, formal lines of authority through new informal relationships among health information proponents in the interest of data security and assurance. These relationships became critical in advancing the broader DHIAP agenda.

As understanding about DHIAP grew in the community, invitations came to participate in other formal activities focused on health information assurance, including the HIPAA Integrated Project Team (the HIPAA IPT) and the Information Assurance Workgroup of OSD/HA. In order to begin coordinating responses to the proposed HIPAA transaction, data security and medical privacy regulations, OSD/HA created a HIPAA Interim Project Team (HIPAA IPT). The HIPAA IPT meets monthly and sponsors work groups on specific issues such as the impact of the transaction standards on various DoD information systems. Sherry McKenzie, the Director of the HIPAA IPT, invited TATRC to appoint a representative of DHIAP to join the HIPAA IPT and contribute to its data security efforts. The HIPAA IPT thus constitutes a forum for presenting and disseminating information about DHIAP's development to a wide audience in DoD and service health information management. The OSD/HA Information Assurance Program and Privacy Office, a participant in the original DHIAP strategic planning meeting meets monthly and includes senior information officers from all the services and many agencies. A representative from DHIAP also attends and routinely briefs these meetings about the project's development.

These three lines of work intersected as the DHIAP sought support for the appointment of the MISRT and launching of the training seminars. The DHIAP included funds to pay transportation and per diem of all MISRT to the training seminars. In order officially to notify MTFs and legitimate the MISRT training seminars, the DHIAP asked senior DoD and service health information management officials to send letters to regional and MTF commanders supporting these activities. After extended discussion among the medical CIO offices, the P3 Workgroup, the HIPAA IPT and other proponents, letters were drafted and staffed to the service surgeons general. The Air Force, Army and Navy surgeons general have signed and sent their letters of support. These letters document and constitute an important product of the emerging Community of Proponents for Health Information Assurance. While the Community of Proponents includes formal structures such as the P3 Workgroup, the HIPAA IPT, and the service medical CIOs, it crosscuts and interweaves such structures together in a network of informal relationships to support and help sustain the broad health information assurance effort.

IV. Conclusion: Metaphors and culture change in healthcare

This paper has described changes in organizations of varying sizes and scales. Such organizational changes notwithstanding, changing culture requires changing the metaphors that inform peoples' understanding of their situation. On this issue, healthcare's recent experience with blood-born pathogens may prove instructive. When healthcare workers initially faced the policies, procedures and practices known as "Universal Precautions", they resisted the changes. Latex gloves slowed them down and reduced sensitivity to touch. Goggles, gowns and clunky syringes made work much more difficult. Nobody had time to attend orientation or annual refresher training in blood-born pathogen controls. Things have changed. Strong enforcement of the regulations and improved technology have helped healthcare workers accept Universal Precautions as part of their everyday work. Another condition underlies their acceptance of these changes, however: a sense of threat. Healthcare workers now all realize and accept that blood-born pathogens pose a serious threat to themselves, their patients and their organizations. When healthcare organizations realize and accept that breaches of health information security also pose serious threats to their employees, patients, business associates and business operations, they will develop cultures that sustain rather than undermine health information assurance.

Acknowledgements

The work of Collmann on this project has been funded in whole or in part with Federal funds from the National Library of Medicine under Contract No. N01-LM-6-3544, and an Interagency Personnel Agreement between Georgetown University Medical Center and the Telemedicine and Advanced Technology Research Center, US Army Medical Research and Materiel Command, Ft. Detrick, MD. Sostrom's work has been funded by the Defense Health Information Assurance program, contract number DAMD17-99C 9001. Opinions, interpretations, conclusions and recommendations are those of the authors and are not necessarily endorsed by the National Library of Medicine or the Department of Defense. The authors wishes to thank their colleagues in the DHIAP, MAJ Cathy Beck, Willie Wright, Chris Alberts, Audrey Dorfee and Neal Neuberger for their support.

References

1. Collmann, J. Cooper, T. Demster, et al. *The CPRI Toolkit: Managing Information Security in Health Care, 2nd Edition* Computerized Patient Record Institute: Bethesda, MD, 1999 and World Wide Web Edition, 3Com: San Jose, CA. 1999, *3rd Edition* Computerized Patient Record Institute: Bethesda, MD, 2000 and World Wide Web Edition, 3Com: San Jose, CA. 2000

2. Collmann, J. Cooper, T. Demster, et al. *The CPRI Toolkit: Managing Information Security in Health Care, 2nd Edition* Computerized Patient Record Institute: Bethesda, MD, 1999 and World Wide Web Edition, 3Com: San Jose, CA. 1999, *3rd Edition* Computerized Patient Record Institute: Bethesda, MD, 2000 and World Wide Web Edition, 3Com: San Jose, CA. 2000

3. Collmann, J. Meissner, M. Tohme, W. Winchester, J. Mun, S. Comparing the security risks of paper-based and computerized patient record systems.*Proceedings, Medical Imaging '97, PACS Design and Evaluation: Engineering and Clinical Issues* SPIE, Newport Beach, CA, 1997; 3035:172-182.

4. Meissner MC, Collmann J, Tohme WG , et al. Protecting Clinical Data in PACS, Teleradiology Systems and Research Environments", *Proc. Soc. Photo-Opt. Instrum. Eng., PACS Design & Evaluation: Medical Imaging,* 1997; 3035.

5. Sostrom, K. Collmann, J. Reviewing and reforming policy in health enterprise information security *Proc. Soc. Photo-Opt. Instrum. Eng., PACS Design & Evaluation: Medical Imaging,* in press.

6. Alberts, C. Behrens, S. Pethia, R.Wilson, W Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} *(OCTAVE^{SM})* Framework, Version 1.0 (CMU/SEI-99-TR-017). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 1999.

7. Alberts, C. Dorfee, A. HIPAA and Information Security Risk: Implementing an Enterprise-Wide Risk Management Strategy, *Proc. Soc. Photo-Opt. Instrum. Eng., PACS Design & Evaluation: Medical Imaging,* in press.

8. United States General Accounting Office. Information Security: Computer Attachs at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84

9. United States General Accounting Office. Department of Defense Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk. GAO/AIMD-99-107

10. Sostrom, K. Collmann, J. Reviewing and reforming policy in health enterprise information security *Proc. Soc. Photo-Opt. Instrum. Eng., PACS Design & Evaluation: Medical Imaging,* in press.

Jeff Collmann, Ted Cooper, B Demster, Kathleen Frawley, Shonna Koss, Bruce Patterson, Paul Schyve, Renee Ornees, The CPRI Toolkit: Managing Information Security in Health Care, 2nd Edition Computerized Patient Record Institute: Bethesda, MD, 1999 and World Wide Web Edition, 3Com: San Jose, CA. 1999, 3rd Edition Computerized Patient Record Institute: Bethesda, MD, 2000 and World Wide Web Edition, 3Com: San Jose, CA. 2000

CPRI TOOLKIT:

Managing Information Security in Health Care

Table of Contents

HIPAA and the Military Health System:
Organizing technological and organizational reform in large enterprises

Jeff Collmann Ph.D

in

Proc. Soc. Photo-Opt. Instrum. Eng., PACS Design & Evaluation: Medical Imaging, in press.

MI 4323-19

HIPAA and the Military Health System: Organizing technological and organizational reform in large enterprises

Jeff Collmann[a], (Georgetown University Medical Center, Washington, DC 20015 and Telemedicine and Advanced Technology Research Center, Ft. Detrick, MD 21702)

ABSTRACT

The global scale, multiple units, diverse operating scenarios and complex authority structure of the Department of Defense Military Health System (MHS) create social boundaries that tend to reduce communication and collaboration about data security. Under auspices of the Defense Health Information Assurance Program (DHIAP), the Telemedicine and Advanced Technology Research Center (TATRC) is contributing to the MHS's efforts to prepare for and comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 through organizational and technological innovations that bridge such boundaries. Building interdisciplinary (clinical, administrative and information technology) medical information security readiness teams (MISRT) at each military treatment facility (MTF) constitutes the heart of this process. DHIAP is equipping and training MISRTs to use new tools including "OCTAVE", a self-directed risk assessment instrument and "RIMR", a web-enabled Risk Information Management Resource. DHIAP sponsors an interdisciplinary, triservice workgroup for review and revision of relevant DoD and service policies and participates in formal DoD health information assurance activities. These activities help promote a community of proponents across the MHS supportive of improved health information assurance. The MHS HIPAA-compliance effort teaches important general lessons about organizational reform in large civilian or military enterprises.

Keywords: HIPAA, social boundaries, interdisciplinary, proponents

1. INTRODUCTION

The data security rules proposed for promulgation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require reconceptualizing the idea and process of compliance. Unlike a set of rules numerable as a checklist of activities and limited to a single domain of endeavor such as infection control, the HIPAA data security rules require the exercise of broad administrative judgement about activities, functions and conditions across multiple domains in a health care enterprise. From an organizational perspective, this means that responsibility for complying with HIPAA must be shared across the enterprise, most particularly among the broad clinical, administrative and information technology fields, and integrated into the enterprise's business culture. How this occurs will vary across the industry depending on the organizational and cultural conditions of specific healthcare entities. The global scale, multiple units, diverse operating scenarios and complex authority structure of the Department of Defense healthcare system create social boundaries that tend to reduce communication and collaboration about data security. Under auspices of the Defense Health Information Assurance Program (DHIAP), a congressionally mandated research project, the Telemedicine and Advanced Technology Research Center (TATRC) is contributing to the efforts of DoD healthcare to prepare for and comply with HIPAA through organizational and technological innovations that bridge such boundaries.

2. THE PROBLEM: BOUNDARIES IN THE DEPARTMENT OF DEFENSE

Multiple conditions create boundaries inhibiting communication, collaboration and coordination about health information assurance (HIA) in the military healthcare system. Although federal laws, federal regulations and DoD provide guidance on HIA policies and procedures, the Air Force, Army, and Navy historically interpret that guidance in ways relevant to their own service traditions and operating conditions. The organization of health information assurance management reflects this relationship between the general and specific at the policy level with the Office of the Secretary of Defense/Health Affairs and the surgeons general respectively representing the DoD and service programs. For both the DoD and services, policies and procedures for information technology, medical records, and clinical care have developed relatively independently. From the perspective of IT policy, health care functions as just another application area with no officially recognized specific needs of its own. In spite of the ubiquity of the Comprehensive Health Care System (CHCS, the military's electronic patient record system) and multiple special applications such as MDIS (the military's computer-based radiology picture archiving system), medical records policy has only just begun to acknowledge the existence of computer-based healthcare records. The clinical, patient administrative and information technology chains-of-command similarly function with little formal regard for each other except at high level points of command. Military medical centers hospitals and ambulatory clinics (known by the acronym, MTF) constitute major points of organizational consolidation that exercise substantial responsibility and authority for many operational functions. With respect to HIA, each MTF must develop its own policies, procedures and practices again drawing guidance from higher directives but exercising discretion to adapt to local conditions. The MTFs represent the unit of compliance for many accreditation and regulatory processes such as JCAHO and HIPAA. In addition to all this complexity, the military health care system faces a variety of different contexts within which it must operate. The military health care system provides services across various "echelons of care" from medical centers in the United States to field clinics in deployment zones for members of the military forces, family members and civilians in both military and civilian treatment facilities. Moreover, information generated in one context often crosses boundaries through a variety of media to another context such as a wounded soldier who gets transferred from a battalion aid station in theater to a medical center well behind the lines. HIPAA implicates this entire spectrum of endeavor.

3. THE APPROACH: BRIDGING ORGANIZATIONAL BOUNDARIES

Two primary objectives of the DHIAP will promote building bridges across these organizational boundaries in the military healthcare system, namely creating, training and equipping interdisciplinary Medical Information Security Readiness Teams (MISRT) at all MTFs and encouraging development of a Community of Proponents of Health Information Assurance interweaving all levels of the military healthcare system. Achieving these two objectives together should incorporate health information assurance into the corporate culture of the military healthcare system thus supporting long term enhancement of medical information security readiness as well as achieving compliance with the HIPAA data security regulations.

3.1 Medical Information Security Readiness Teams

In letters sent to regional medical commands, MTF commanders and others, the surgeons general of the Army and Navy directed appointment at all MTFs in the world of a HIPAA focal point and implementation team composed of three people representing the clinical, patient administrative and information technology fields. Developing the MISRT teams recognizes two important points: 1) medical commanders at MTFs bear ultimate responsibility for complying with the HIPAA data security regulations, and 2) the security of MTF information systems touches clinical and administrative work as well as the work of information technologists. Hence, representatives of all these fields should share responsibility for developing the MTF's approach to health information assurance.

The surgeons general also recommended that the teams attend training seminars on the content of and new tools for complying with the proposed HIPAA regulations being sponsored by TATRC and the Chief Information Officers of the Military Healthcare System. A discussion of the seminar agenda follows below. Please note two important points about the process. First, in order to build and create support for the MISRT, TATRC organized the training seminars on a regional basis. MISRT from all Air Force, Army and Navy MTF in each region attended a seminar together in a single location within their own region. For example, all MISRT in Region 1 including MTFs from Maryland, Delaware, Pennsylvania, New Jersey, New York, and all the states of New England attended a seminar in Bethesda, Maryland on January 26, 2001. Two, during the seminars, the MISRT worked together in breakout sessions. By jointly conducting exercises in policy review and risk assessment, the attendees get to know the members of their own MISRT and members of MISRT from other MTF. These exercises thus stimulate emergence of a regional community of practice with members from all MTFs, each military service (Air Force, Army and Navy) and each discipline (clinical, administrative, and IT). The DHIAP will continue supporting the local MISRT and regional communities of practice with follow-up training and a web-enabled, knowledge management portal named "RIMR" (see description below). The MISRT and the regional communities of practice should mitigate a primary threat to health information assurance: relegation of responsibility for information security to IT staffers operating in isolation from other staff at their own and other MTFs.

The training seminars also introduced MISRT to new policy analysis and risk management tools developed under the auspices of the DHIAP research effort. As described by Kristen Sostrom elsewhere in this program, DHIAP sponsors an interservice, interdisciplinary Policy, Procedure and Practices (P3) Workgroup to compare all relevant Department of Defense and individual service regulations with the HIPAA data security regulations. As part of this process, the P3 Workgroup developed various templates, matrices and report forms to conduct, document and analyze the results of the HIPPA-DoD policy comparison. The MISRT will similarly have to assess their own MTF policies as part of their HIPAA compliance efforts. During the seminar, Ms. Sostrom instructs the MISRT in the HIPAA regulations and introduces them to the P3 tools. The MISRT practice using the tools by reviewing and revising their MTF information access policies during the first breakout session.

During the afternoon session, the MISRT learn about two key tools being developed and implemented by the DHIAP, a web-enabled Risk Information Management Resource (RIMR) and a self-directed information risk assessment tool called "OCTAVE". As described by Chris Alberts elsewhere in this program, OCTAVE enables the MISRT to discharge the central activity required by HIPAA, develop a health information security risk management plan[1]. As MISRTs begin implementing their risk management plans, they will require a variety of types of information about information security, including policy documents, risk databases, and technology reports. Using advanced computerized knowledge management tools, RIMR will consolidate and make such resources available to MISRT via the world wide web. OCTAVE sits on RIMR and eventually will link to RIMR risk assessment databases through a direct entry GUI. EASEL, an information security simulation language also being developed under DHIAP, will also reside on RIMR. With respect to supporting the regional communities of practice, RIMR includes tools for creating regional and national webboards through which MISRT can query each other about security issues and share their experiences.

3.2 Community of Proponents for Health Information Assurance

Creating, training and equipping MISRT establishes new formal structures at the MTF level for managing health information assurance. The DHIAP has also worked to develop informal new relationships that interweave formal DoD and service chains-of-command, agencies and operational levels in support of health information assurance. Given the relatively amorphous but nonetheless real impact of these informal relationships, we designate this emerging support network a Community of Proponents for Health Information Assurance. Like the Internet itself, the Community of Proponents will never exist as a defined structure with formal roles or boundaries. No Program Executive Officer will call a meeting of the Community of Proponents to take action on a security breach. Rather, the Community of Proponents addresses problems such as the lack of command support for information assurance. According to the GAO, commanders at all levels remain relatively indifferent to threats and vulnerabilities in the US defense computer network[2, 3.] Although one should focus attention on commanders themselves with new policies, increased indoctrination, and perhaps disciplinary action, such measures would fail to address the organizational conditions under which any member of the military practices or ignores sound information security discipline in their everyday work. Broad agreement, high expectations and routine good practice of health information assurance must exist woven into the structure of informal relationships that authoritatively govern and execute the chores of daily life. A discussion of efforts to disseminate information and build support for the DHIAP will illustrate these points.

Three lines of work have helped build support for the DHIAP, including executing an ongoing series of briefings about the project, sponsoring a triservice, interdisciplinary policy review called the Policy, Procedure and Practice (or, P3) Workgroup and participating in formal committees of the Office of Health Affairs. Because of the imminent need to comply with HIPAA and the range of health information assurance issues faced by the military health system, many agencies have an interest in the DHIAP. Since July 1999, we have consequently responded to requests for and, in some cases, initiated briefings about the aims and ongoing accomplishments of the project. We initiated this line of work by inviting representatives of critical agencies in the DoD and US Army information assurance effort to a strategic planning meeting in July 1999. Representatives from Office of the Secretary of Defense/Health Affairs (OSD/HA), the US Army Surgeon General, US Army Theater Information Management Program Office (TIMPO), the Information Assurance Technical Assistance Center (IATAC) and TATRC participated. This meeting produced agreement on key strategic thrusts for DHIAP, including development of a self-directed risk assessment tool (what became OCTAVE), a medical information assurance simulation tool, a method and examples of technical business case analyses for information assurance technology, a policy review initiative, a web-enabled knowledge management tool to make these tools available (RIMR) and a major educational effort to help MTFs enhance health information practice and prepare for HIPAA. The meeting also decided that the DHIAP's work should be expanded beyond its originally base in the Army to include the DoD, the Air Force and the Navy. A single theme underlies these strategic thrusts, namely maximizing the ability of MTFs to manage health information assurance at the local level.

We consolidated these decisions into a strategic research plan, initiated the work and began briefing proponents in DHIAP's development. After briefing commanders at TATRC and the US Army Medical Research and Materiel Command at Ft. Detrick, we initially briefed Mr. Reardon, the Chief Information Officer and Designated Accreditation Agency, OSD/HA. We have subsequently briefed the Chief Information Officers of each medical service, the office of the US Army Director of Information Security Command, Control, Communications, and Computers (DISC4), the Information Assurance Program and Privacy Office, and others. We are refining and adapting the DHIAP strategic research plan in response to emerging DoD and service health information assurance needs as this process unfolds.

The July 1999 meeting recommended initiating a review of DoD and service level policy on all aspects of health information assurance in light of the proposed HIPAA data security regulations. We realized that HIPAA posed a challenge to standard DoD practice in policy development for information assurance. HIPAA takes an integrated approach to data security requiring coordination of administrative and technical work. From a policy perspective that means cross-referencing policies in medical records management and computer security. We also recognized that HIPAA offered an opportunity for interservice collaboration in policy development. With these ideas in mind, we developed the Policy, Procedure and Practice (P3) Workgroup. The initial meeting included the chief medical records officers from the Air Force, Army and Navy Surgeons General offices, a representative of OSD/HA and TATRC. After conducting a preliminary analysis of medical records policies, the group decided also to seek representation of the information technology communities of each service. Thus the P3 Workgroup became an interdisciplinary and interservice activity.

The P3 Workgroup adopted a work process designed to take maximum advantage of its interdisciplinary, interservice composition. After working as a committee of the whole to develop and learn a joint approach to policy review, the P3 Workgroup split into two subgroups to work more quickly. One group included all representatives of the Navy and OSD/HA. The other group included the Army and Air Force representatives. TATRC representatives participated in both groups. These groups conducted exhaustive primary comparisons between the HIPAA data security rules and all pertinent policies of their respective services. After completing this primary review using tools described elsewhere by Kristin Sostrom, each subgroup conducted a quality assurance review of the work of their counterparts in the other subgroup. While this core dialogue and work produced an analysis of policies, it simultaneously linked distinct, formal lines of authority through new informal relationships among health information proponents in the interest of data security and assurance. These relationships became critical in advancing the broader DHIAP agenda.

As understanding about DHIAP grew in the community, we received invitations to participate in other formal activities focused on health information assurance, including the HIPAA Integrated Project Team (the HIPAA IPT) and the Information Assurance Workgroup of OSD/HA. In order to begin coordinating responses to the proposed HIPAA transaction, data security and medical privacy regulations, OSD/HA created a HIPAA Interim Project Team (HIPAA IPT). The HIPAA IPT meets monthly and sponsors work groups on specific issues such as the impact of the transaction standards on various DoD information systems. Sherry McKenzie, the Director of the HIPAA IPT, invited TATRC to appoint a representative of DHIAP to join the HIPAA IPT and contribute to its data security efforts. The HIPAA IPT thus constitutes a forum for presenting and disseminating information about DHIAP's development to a wide audience in DoD and service health information management. The OSD/HA Information Assurance Program and Privacy Office, a participant in the original DHIAP strategic planning meeting meets monthly and includes senior information officers from all the services and many agencies. A representative from DHIAP also attends and routinely briefs these meetings about the project's development.

These three lines of work intersected as the DHIAP sought support for the appointment of the MISRT and launching of the training seminars. The DHIAP included funds to pay transportation and per diem of all MISRT to the training seminars. In order officially to notify MTFs and legitimate the MISRT training seminars, the DHIAP asked senior DoD and service health information management officials to send letters to regional and MTF commanders supporting these activities. After extended discussion among the medical CIO offices, the P3 Workgroup, the HIPAA IPT and other proponents, letters were drafted and staffed to the service surgeons general. As of this writing, the Army and Navy surgeons general have signed and sent their letters of support. The Air Force is finalizing its letter. These letters document and constitute an important product of the emerging Community of Proponents for Health Information Assurance. While the Community of Proponents includes formal structures such as the P3 Workgroup, the HIPAA IPT, and the service medical CIOs, it crosscuts and interweaves such structures together in a network of informal relationships to support and help sustain the broad health information assurance effort.

4. Conclusion: Promoting a Culture of Health Information Assurance

Preliminary analysis of our experience with the military healthcare system suggests that developing a culture of health information assurance requires the complex interaction of three levels of work, namely data security-related activities, organizational functions supporting data security and organizational conditions that sustain and/or undermine data security. By activities, we mean all those tasks and programs that organizations accomplish in the name of improving the security of health information such as assessing risk, auditing logbooks, sponsoring training, and investigating security incidents. Organizations frequently sponsor activities while discharging broad functions that support data security such as monitoring changing regulations, laws and professional standards and continuously reviewing, revising and enforcing data security policies, procedures and practices[4, 5.] Sustaining such security-related activities and functions, however, requires organizations to bridge social boundaries that tend to reduce communication and collaboration about data security among their constituent units. The DHIAP has helped promote a culture of health information assurance in the military healthcare system by developing new tools to discharge security functions better at the MTF, by sponsoring reviews of policy and procedure, and, critically, by developing new formal and informal structures bridging boundaries between disciplines, services, chains-of-command and units of organization through the MISRT and the Community of Proponents.

ACKNOWLEDGEMENTS

The Defense Health Information Assurance Program, contract number DAMD17-99C 9001, supports the research upon which this paper is based. Opinions, interpretations, conclusions and recommendations are those of the authors and are not necessarily endorsed by the Department of Defense. The author wishes to thank his colleagues in the DHIAP, MAJ Cathy Beck, Willie Wright, Kristen Sostrom, Chris Alberts, and Archie Andrews for their support and insight into health information assurance. Seong K. Mun makes the work possible by sustaining the ISIS Center as a home for odd ducks swimming furiously.

REFERENCES

1. Christopher J Alberts,.; Behrens, Sandra G.; Pethia, Richard D.; & Wilson, William R. *Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) Framework, Version 1.0* (CMU/SEI-99-TR-017). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 1999.
2. United States General Accounting Office. *Information Security Risk Assessment, Practices of Leading Organizations* (GAO/AIMD-00-33). Washington, D.C.: GAO, November 1999.
3. United States General Accounting Office. *Information Security Risk Assessment, Practices of Leading Organizations* (GAO/AIMD-00-33). Washington, D.C.: GAO, November 1999.

4. Jeff Collmann and Anna-Lisa Silvestre, Building a Security Capable Organization, Proceedings, PACMedTek, IEEE Computer Society, Washington, DC 1998.
5. Jeff Collmann, Ted Cooper, B Demster, Kathleen Frawley, Shonna Koss, Bruce Patterson, Paul Schyve, Renee Ornees, *The CPRI Toolkit: Managing Information Security in Health Care*, 3rd Edition Computerized Patient Record Institute: Bethesda, MD, 2000 and World Wide Web Edition, 3Com: San Jose, CA. 2000

Telemedicine for Rehabilitation

Project Description

Cognitive Behavioral Therapy (CBT) has been found to be efficacious in the treatment of people who need to manage multiple physical symptoms associated with the spectrum of illnesses known as Chronic Multi-symptom Illnesses (e.g., Fibromyalgia, Chronic Fatigue, and Gulf War Veterans Illnesses). CBT (normally conducted face-to-face and in a small group format) is known to reduce pain, increase function, and improve quality of life among these sufferers. Our goal is to test out possible ways to deliver CBT treatment (in small groups) at a distance using videoconferencing technology, with an adjunctive Web site for conveying the CBT material (normally handed out in the form of a participant manual) and homework assignments. Evaluation data was collected via this site on a weekly basis during treatment, and monthly during follow-up periods (3 months, 6 months). Pilot testing was aimed at finding out how to optimize distance group therapy (i.e., length of each session, length of treatment duration, size of group) and to see whether participants felt adequately satisfied with this medium.

Five groups were conducted by either one of two therapists, beginning in June 2000, to pilot varying lengths of treatment (2 groups experienced 90 minute sessions weekly for 6 sessions, 1 group received 60 minute sessions for 6 weekly sessions, 1 group received 14 sessions weekly, and another group received 12 sessions weekly). The clinical psychologists transmitted from one location (via 2 ISDN lines, Polycom systems, and a Vizcam that enabled display of written material) and interacted with a group of 4 participants who sat at a table face-to- face. Subjects were referred by Rheumatologists from 1 of 2 sites, Lewes Delaware or Georgetown University in Washington DC.

Project Outcomes

Extensive pre and post measures were collected (pending formal analysis) regarding satisfaction, physical functioning, mood, and pain. Preliminary (qualitative) results suggest that participants' first preference would be for traditional face-to-face therapy with the therapist in the room. However, if that would be improbable due to lack of access to therapy in their locale, participants appeared to largely tolerate distance group therapy adequately. Though there were outliers. One participant (who had participated in several years of different types of therapy) mentioned she preferred the distance because it seemed as though she didn't have to be as concerned about socializing before the session with the therapist. Another participant felt that this format seemed too impersonal to feel connected to the therapist. However, most indicated they felt they had adequate rapport with the therapist, despite the distance. Though they were aware of time delays in voice and video, limited ability to see facial nuances in video, and some unusual practices for relating with the therapist (i.e., participants might raise their hand to speak instead of more natural interactions), most participants indicated that the "distance" was not a significant barrier to getting their psychological needs met. The two therapists both indicated that videoconferencing did not appear to significantly obstruct their ability to conduct group therapy.

Preliminary qualitative data suggests certain optimal conditions, to include: (1) 90 minute sessions, (2) 8 weekly sessions, (3) 1 time per week web site login - to access material, homework, and complete the assessment, (4) 4 persons per group at one site, (5) video quality is less important, good quality audio is necessary (6) a 20 to 30 minute pre-group individual phone call from therapist to participant appears to be sufficient for establishing initial rapport (It has been suggested in telepsychiatry literature that it might be best to meet face-to-face with patients before going to videoconferencing). (7) A group activity was designed to increase group cohesion, to bridge the gap of the unusualness of distance therapy (Because participants can become less engaged among themselves when they focus on the psychologist, seen in the monitor, group cohesion seemed to develop less naturally in this setting than in traditional group CBT.) (8) Adequate computer literacy needs to be verified (using a behavioral test of knowledge) before allowing participation. (9) Special computer-related issues need to be covered within the first session, including confidentiality issues surrounding shared computer usage at home or sharing participant's email addresses.

We feel ready to proceed with the actual randomized control trial, except for one remaining issue. We'd intend to run additional pilots to test IP-based videoconferencing (in place of ISDN) to conserve resources and to make groups even more accessible. We've identified a much more portable and universal system which we believe will cost a small fraction of the ISDN-based system. Though we believe the quality of the audio and video are equally adequate to meet therapeutic needs, this will need to be verified.

Potential Benefits

(1) Increased access of CBT for management of CMI
(2) Standardized treatment delivered by 'experts' in the field
(3) Portability (access will be available via a laptop/internet connection)
(4) Group social support provided to people in isolated locales
(5) A generic distance-therapy model for self-management of most chronic illnesses

Success to date

Items (1-9) under outcomes section are the preliminary necessary information for understanding the treatment 'basics' before proceeding to a full-fledged trial.

Challenges

(1) Perhaps IP-based videoconferencing will be more 'fickle' due to network glitches and uncontrollable variables, like WWW traffic jams.

(2) Self-management for any illness or change of any maladaptive behavior takes practice over the long term. Relapse back to old ways of behaving is currently the norm. We hope that by utilizing the Web site as a forum for long term social support among participants who have learned the appropriate skills, we may provide an innovative resource for the age-old medical problems related to adherence/compliance to medical regimens.

Military Significance

Traditional CBT involving patient-therapist contact has been shown to be successful in improving the health status of persons with chronic multisymptom illnesses. These illnesses are a significant problem for DoD, especially following military deployments (e.g. Gulf War Veterans Illnesses). Unfortunately in DoD and other large health care systems the number of therapists trained in CBT is small compared to the number of potential patients. The successful use of CBT using teleconferencing and web-based instruction could lead to greater application of the treatment to more DoD patients.

GEORGETOWN UNIVERSITY

TECHNICAL REPORT

"NAIROBI TELEMEDICINE PROJECT"

June 5, 2000

Principal Investigator: Seong K. Mun, Ph.D.
Professor of Radiology and Director of ISIS Center
Georgetown University Medical Center
2115 Wisconsin Avenue, NW, Suite #603
Washington, DC 20007

NAIROBI TELEMEDICINE PROJECT

TABLE OF CONTENTS

MONTHLY TECHNICAL REPORT
FOR
"NAIROBI TELEMEDICINE PROJECT"

Contract Number: S-LMAQM-99-D-0116

Period of Performance: **May 1 - 31, 2000**

1. Work Accomplished in This Reporting Period

1.1. Management and Engineering Support

– In preparation for the Pathfinder Project issues regarding the compatibility, security and network compliance of the telemedicine system to the OPEN-Net environment were discussed at several project meetings at MED on May 2nd, 3rd and May 12th 2000 participated by MED, Georgetown University and IRM. Pertinent technical issues brought up during the meetings are listed in the bullets below with responses to questions below. Before the Pathfinder Project proceeds with it's pilot program, decision was made to prepare and test the telemedicine platform selected under a network simulated environment to be provided by IRM. Preparation were undertaken by Georgetown to support these activities.

- Specifics of the client/server architecture:
  VIEWSEND™ Medical is not a client/server system. Image transfer, annotation and collaboration are on a peer-to-peer basis. KLT has designs for a client/server architecture that is available from one of their OEMs.
- Type of connection necessary – "session to session"? Other?
  Connection type is based on available bandwidth at the post. Complete study information may be transmitted via email. When opened, the email meshes seamlessly with the recipient's database. Email takes advantage of least cost routing to OpenNet locations and off-net locations. Connections may be resolved using DHCP and a Name server or static IP Addresses. Audio connections are available with as little as 16kbps of bandwidth. Minimum data channel for collaboration is 6kbps. Minimum channel to support

Video/Audio/Data is 64kbps. File transfer via FTP takes advantage of whatever bandwidth is available.

- Sample size of files

  The size of a study is directly proportionate to the complexity of the content and the level of compression used in saving the file. A typical full chest x-ray digitized at 150DPI and 12-bit depth may easily require 1.8MB of storage. With only modest compression, the image can be stored and transmitted using 900kb of space or less. Wavelet compression may provide as much as 30 to 1 compression JPEG Lossless compression is considered to be 2 to 1 JPEG Lossy compression is user adjustable with unacceptable degradation occurring at about 12 or 16 – 1. Other typical image sizes:

  - □ Single frame MRI – 300kb
  - □ Small x-ray (e.g. hand) 35kb
  - □ JPEG dermoscopic (or other video) image – 3kb
  - □ Study demorgraphics – 3k

  Recorded voice annotation 8kb per second recorded.

- Specifications of COTS software to be used for the transactions

  Software that has a direct bearing on the operation of VIEWSEND Medical:

  - □ Data Access Objects Version 3.50
  - □ VCON MeetingPoint SDK distribution version 4.01
  - □ Microsoft Netmeeting 2.1(4.3.2203)
  - □ Microsoft Internet Explorer Ver 4.X
  - □ VIEWSEND™ Medical Version 7.0.162
  - □ EZ-SCSI 5.0
  - □ TWAIN for VIDAR Scanner 4.23
  - □ User's choice of email software that is MAPI compliant.
  - □ Windows NT 4.0 Workstation with Service Pack 4

- Encryption strategies, if any, for the system

  The encryption strategy for VIEWSEND Medical systems is based on the standard Public-Key/Symmetric-Key encryption methodology. As an example of a store and forward transmission using email, all patient information and medical imaging are packaged, compressed, and then encrypted with a private 128-bit key. This private is used at the receiving site to decrypt and retrieve the patient medical data. In addition, KLT offer's TopSecret IP™ encryption package in collaboration with VCON. TopSecret IP™ – is add-on software for all KLT AND VCON's IP-based products. TopSecret IP™ provides high quality security against both unauthorized participation and eavesdropping during videoconferences over your IP networks.

- Updated the inventory of communication and computer equipment for Nairobi Health Unit and MED Center (Appendix A).
- Created a communication and computer equipment inventory for the new KLT equipment (Appendix B).
- Updated the project task schedule and time chart of Nairobi Telemedicine Project according to work accomplished and work pending (Appendix C).
- Supplied MED with supporting documentation for previously submitted Monthly Technical Reports (Appendix D).
- Provided MED Center with technical documents for the project planning of Pathfinder Project (Appendix E).
- Provided MED with Teleconsulting Operation manual (Appendix F).

1.2. Coordination and Technical Operations Support

- Continued the configuration and testing of the new KLT equipment at MED. According to DoS recommendation during the project meeting (5/12/2000) the videoconferencing, modem connection, speakers and microphone functions are to be disabled from VIEWSEND Medical application before deployment.
- Retrieved two new KLT equipment from MED back to ISIS Center to conduct further software installation. New software installed in the new workstations are:
  - Norton AntiVirus
  - Microsoft Outlok98
  - Paint Shop Pro.
  - Windows Media Player Version 6.4

This page left blank intentionally

- Configured a third new KLT machine according to DoS security guidelines in preparation for the network testing scheduled next month at DoS and installed the software mentioned above.
- Tested functionality on all three new KLT machines for scheduled testing next month on network simulation at 19.6 KBps, 64 KBps, and T1 network speed at DoS.
- Continue to support Mr. George Mimba to solve the Vidar film digitizer problem. After discussing the trouble Nairobi Health Unit facing with the film digitizer with the vender (Appendix G) they couldn't resolve the issue and they redirected us to KLT Telecom, Inc. Work with KLT is pending to resolve the film digitizer issue as soon as possible.

2. Deliverables /Products Produced

- Teleconsulting Operation manual.
- Supporting documents for previously submitted Monthly Technical Reports.
- Supporting documents for Pathfinder Project.

3. Work expected Next Period

- Conduct network testing for three of the new KLT equipment at IRM of DoS.
- Configure, test, and install software on rest of the new KLT equipment.
- Prepare deliverable documents for MED.

4. Summaries and Near-Term Recommendation

Preparations were undertaken in both technical and management aspects for the Pathfinder Project. In addition to Nairobi for the pilot sites, Yaounde of Cameroon and Dar es Saleem of Tanzania are selected for Phase I deployment followed by Port-au-Prince of Haiti, Santo Domingo of Dominican Republic, and Fort Lauderdale in Phase II. New telemedicine platforms purchased for Pathfinder Project were prepared to meet the requirements of the OPEN-NET configuration and security issues. The functionalities of store-and-forward via email attachment will be tested under a simulated OPEN-NET environment with different transmission capacities will be tested with IRM of DoS in the next period.

Appendix A: Inventory of Communication and Computer Equipment

TELEMEDICINE – DOS INVENTORY:

EQUIPMENT NAME	MODEL NO.	SERIAL NO
KLT PC (CPU)	WDAC22100	GUIDBO60196
HITACHI SUPERSCAN ELITE 802 MONITOR	CM800U511	0505856576635N
CANON COMMUNICATION CAMERA + POWER ADAPTER	VC-C1 MK II	50370259
HUB	LinkSys Etherfast	952005761KDH5FB
POLYCOM SOUND PORT PC SPEAKER + POWER ADAPTER	Sound point PC	4D01700192
Mouse	PS2	02439303
Key Board	RS6000	E 004111162066A
NT1 ACE	ADLRAN	F 721A5659

TELEMEDICINE - NAIROBI INVENTORY:

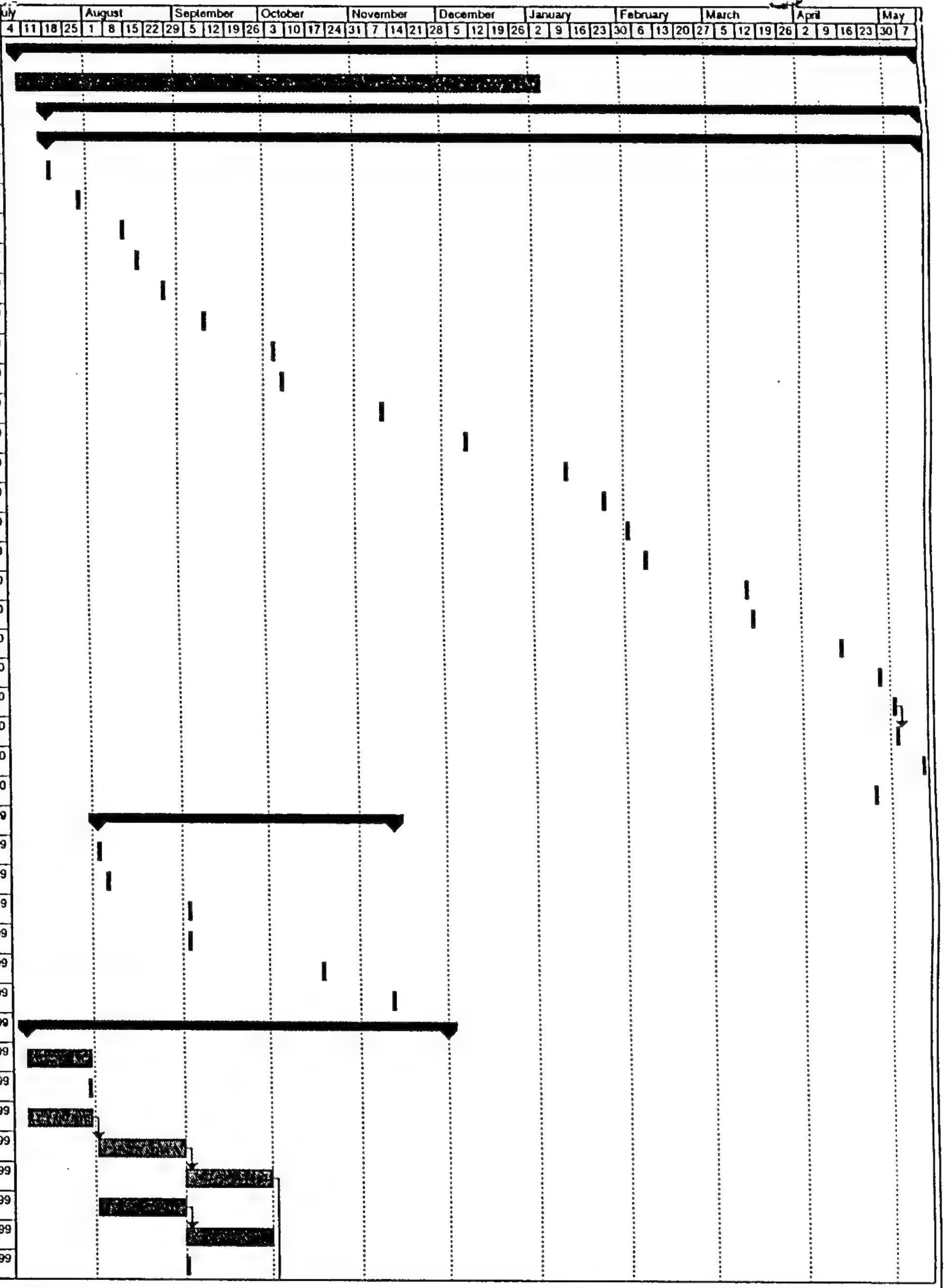
EQUIPMENT NAME	MODEL NO.	SERIAL NO
KLT PC (CPU)	WDAC22100	96112
HITACHI SUPERSCAN ELITE 802 MONITOR		G6H004427
VIDAR COM VXR-12 PLUS FILM DIGITIZER	VXR-12+	24009
CANON COMMUNICATION CAMERA + POWER ADAPTER	VC-C1 MK II	60970358
CANON OPTURA DIGITAL CAMERA + POWER ADAPTER		
AMD MACHINE	AMD-300S	EN 100628
DERMASCOPE		
MICROTEK SCANMAKER E3 PLUS	MRS-600EX3S	87S1523593
MICROPHONE SPEAKER		
POLYCOM SOUND PORT PC SPEAKER + POWER ADAPTER	BARCODE NO. 4D01700171	
TWO REMOTE CONTROLS		
APC SMART-UPS		NS9824017021
TWO POWER STRIPS (EXT. CORDS)		
IP address 10.134.192.24	Gate Way 254	Email VTCNairobi
George Tel 254-2-537-800 Ext3912	Telemedicine WorkStation	254-2-537-808

Appendix B: Inventory of the New KLT Equipment

Delivered	Computer Name	Main Unit	Monitor S-N / M-N	Camera	Location	Features	Peripherals
5/2/2000	KLT 000	23nrk64	55-5319 / IBM 6650-23	109601/ CCD Tele camera	DOS	488MHZ 130MB 2 HDD: 7.86GB Each	WINNOV, VCON, SCSI
5/2/2000	KLT 001	23nrk42	55-53157 / IBM 6650-23	109601/ CCD Tele camera	DOS	488MHZ 130MB 2 HDD: 7.86GB Each	WINNOV, VCON, SCSI
5/5/2000	KLT 002	23nrl77	55-53164 / IBM 6650-23	109601/ CCD Tele camera	ISIS	488MHZ 130MB 2 HDD: 7.86GB Each	WINNOV, VCON, SCSI
5/5/2000	KLT 003	23nrp37	55-53158 / IBM 6650-23	109601/ CCD Tele camera	ISIS	488MHZ 130MB 2 HDD: 7.86GB Each	WINNOV, VCON, SCSI
5/5/2000	KLT 004	23nrg02	55-53161 / IBM 6650-23	109601/ CCD Tele camera	ISIS	488MHZ 130MB 2 HDD: 7.86GB Each	WINNOV, VCON, SCSI

Appendix C: Project Schedule and Time Chart

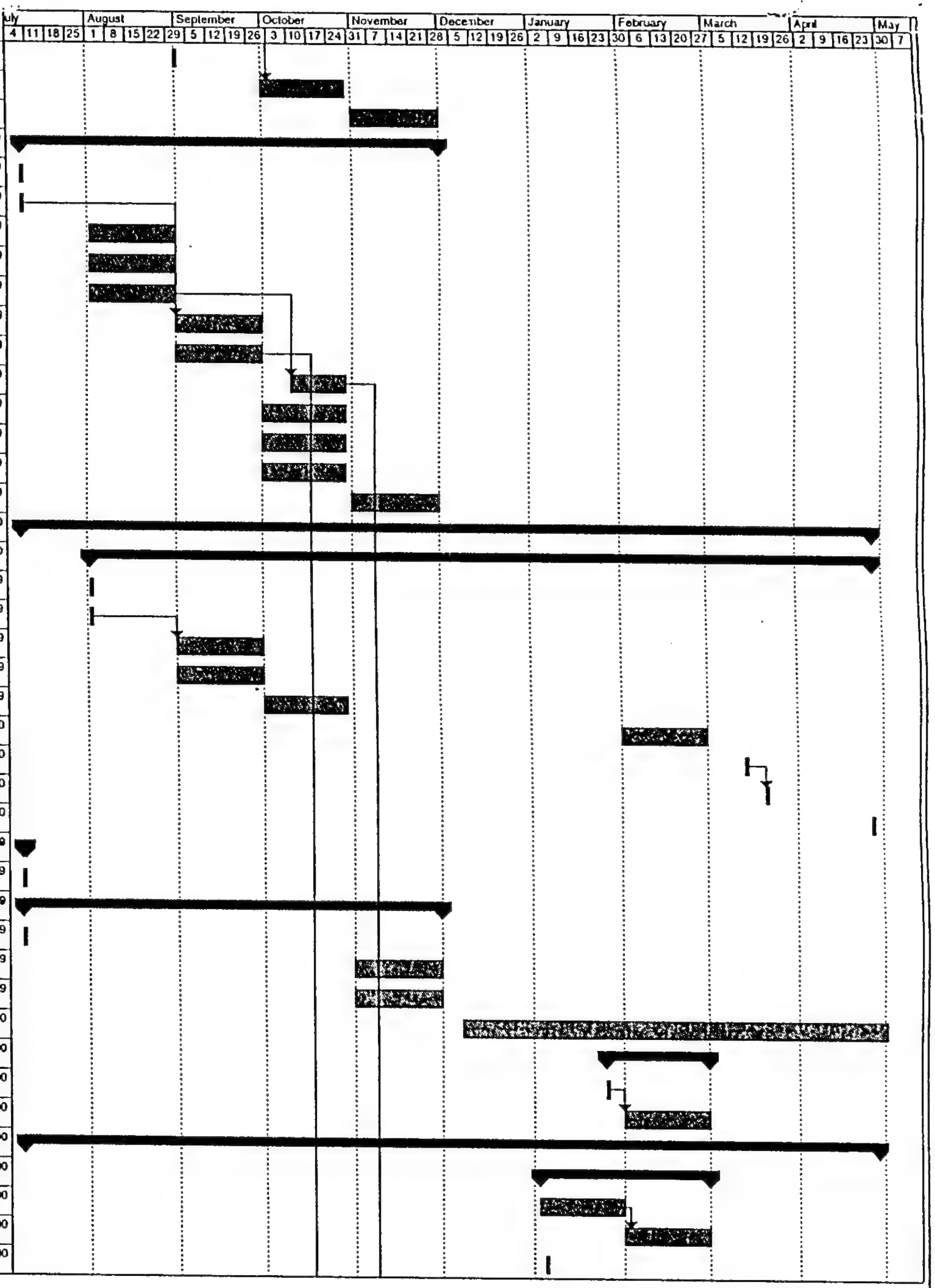
ID	Task Name	Duration	Start	Finish
1	Project Management Support	222 days	Fri 7/9/99	Fri 5/12/00
2	Contact list	129 days	Fri 7/9/99	Tue 1/4/00
3	Project plan	216 days	Mon 7/19/99	Fri 5/12/00
4	Project coordinating meeting	216 days	Mon 7/19/99	Fri 5/12/00
5	Project Meeting at the Department of State	1 day	Mon 7/19/99	Mon 7/19/99
6	Project Meeting at the Department of State	1 day	Thu 7/29/99	Thu 7/29/99
7	Project Meeting at the Department of State	1 day	Fri 8/13/99	Fri 8/13/99
8	Project Meeting at the Department of State	1 day	Wed 8/18/99	Wed 8/18/99
9	Project Meeting at the Department of State	1 day	Fri 8/27/99	Fri 8/27/99
10	Project Meeting at the Department of State	1 day	Fri 9/10/99	Fri 9/10/99
11	Project Meeting at the Department of State	1 day	Mon 10/4/99	Mon 10/4/99
12	Project Meeting at the Department of State	1 day	Thu 10/7/99	Thu 10/7/99
13	Project Meeting at the Department of State	1 day	Wed 11/10/99	Wed 11/10/99
14	Project Meeting at the Department of State	1 day	Thu 12/9/99	Thu 12/9/99
15	Project Meeting at the Department of State	1 day	Wed 1/12/00	Wed 1/12/00
16	Project Meeting at the Department of State	1 day	Tue 1/25/00	Tue 1/25/00
17	Project Meeting at the Department of State	1 day	Wed 2/2/00	Wed 2/2/00
18	Project Meeting at the Department of State	1 day	Tue 2/8/00	Tue 2/8/00
19	Project Meeting at the Department of State	1 day	Mon 3/13/00	Mon 3/13/00
20	Project Meeting at the Department of State	1 day	Wed 3/15/00	Wed 3/15/00
21	Project Meeting at the Department of State	1 day	Fri 4/14/00	Fri 4/14/00
22	Project Meeting at the Department of State	1 day	Thu 4/27/00	Thu 4/27/00
23	Project Meeting at the Department of State	1 day	Tue 5/2/00	Tue 5/2/00
24	Project Meeting at the Department of State	1 day	Wed 5/3/00	Wed 5/3/00
25	Project Meeting at the Department of State	1 day	Fri 5/12/00	Fri 5/12/00
26	Project Meeting at the Department of State	1 day	Tue 4/25/00	Tue 4/25/00
27	Meetings to ensure clear communication with all participants in the Telemedicine service	75 days	Tue 8/3/99	Fri 11/12/99
28	Video Conference with Nairobi at ISIS Center	1 day	Tue 8/3/99	Tue 8/3/99
29	Video Conference with Nairobi at ISIS Center	1 day	Fri 8/6/99	Fri 8/6/99
30	Video Conference with Nairobi at State Department	1 day	Fri 9/3/99	Fri 9/3/99
31	Phone Conference with Nairobi at ISIS Center	1 day	Fri 9/3/99	Fri 9/3/99
32	Brought Mr. Mimba from Nairobi to the DoS to open tech communication	1 day	Tue 10/19/99	Tue 10/19/99
33	Brought two nurses from Nairobi to DoS to open clinical communication	1 day	Fri 11/12/99	Fri 11/12/99
34	Installation of equipment in Nairobi	104 days	Fri 7/9/99	Tue 11/30/99
35	Visited the new U.S. Embassy building to identify requirement infrastructure	16 days	Fri 7/9/99	Fri 7/30/99
36	Coordinate and support moving Telemedicine equipment	1 day	Fri 7/30/99	Fri 7/30/99
37	Coordinate and support installation of ISDN line to the new building	16 days	Fri 7/9/99	Fri 7/30/99
38	Coordinating ISDN install	22 days	Mon 8/2/99	Tue 8/31/99
39	Speed up the ISDN install in the new Health Unit	23 days	Wed 9/1/99	Thu 9/30/99
40	Inquired about an INMARSAT	22 days	Mon 8/2/99	Tue 8/31/99
41	Tested using INMARSAT satellite with KLT Telemedicine system	23 days	Wed 9/1/99	Thu 9/30/99
42	Upgrade the operating system of the Telemedicine unit in MED to MS NT	1 day	Wed 9/1/99	Wed 9/1/99



Project: NairobiTelemedicineProject2
Date: Fri 6/16/00

Task	▨	Progress	▬	Summary	▬	Rolled Up Split	....	Rolled Up Progress	▬	Project Summary	▬
Split	....	Milestone	◆	Rolled Up Task	▨	Rolled Up Milestone	◇	External Tasks	▨		

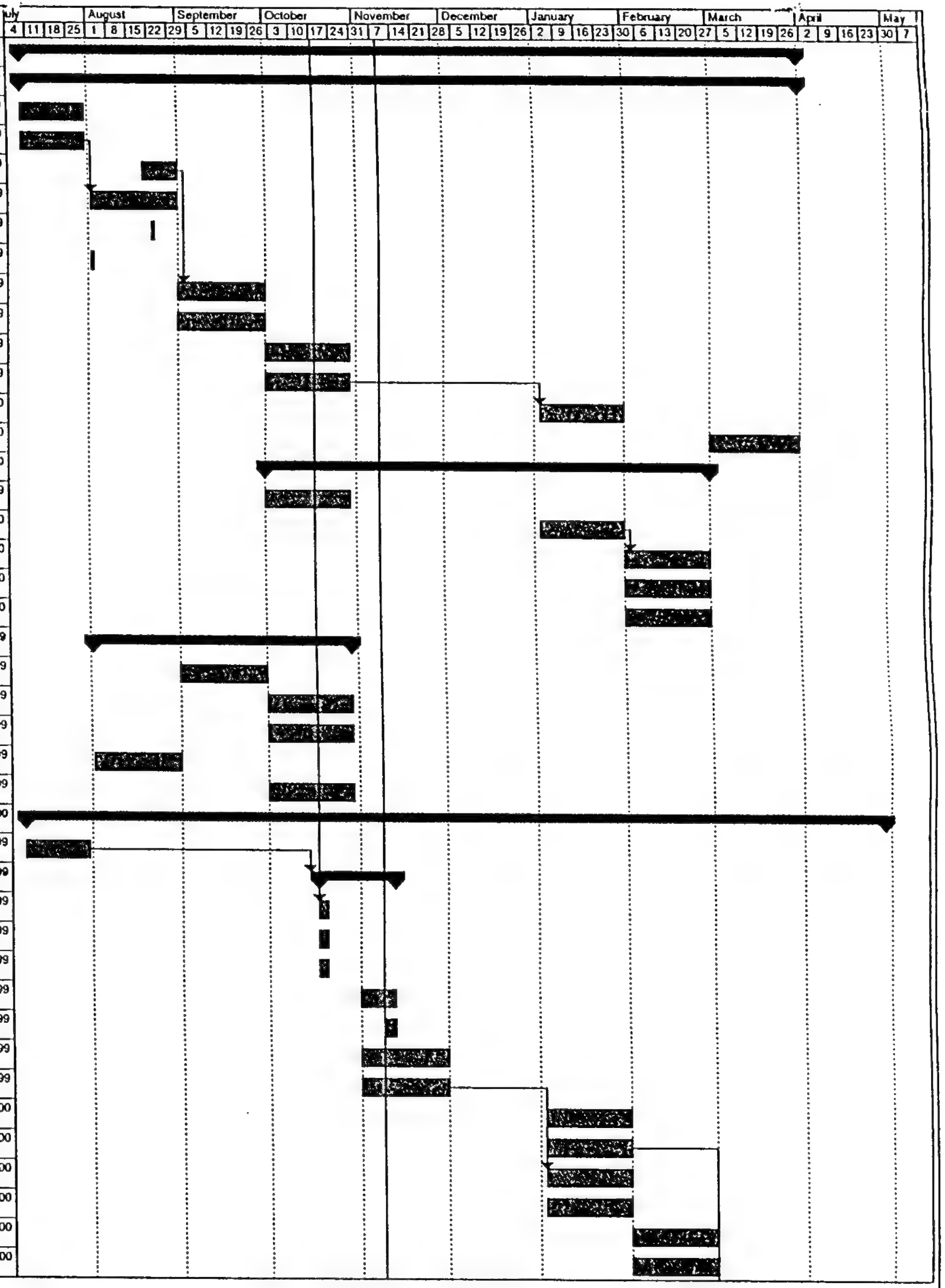
ID	O	Task Name	Duration	Start	Finish
43		Upgrade the operating system of the Telemedicine unit in Nairobi to MS NT	1 day	Wed 9/1/99	Wed 9/1/99
44		Follow-up with the National Postal Office	21 days	Fri 10/1/99	Fri 10/29/99
45		Delay the upgrade of the Telemedicine unit in Nairobi	22 days	Mon 11/1/99	Tue 11/30/99
46		Training plan and schedule for Nairobi	104 days	Fri 7/9/99	Tue 11/30/99
47		Train Mr. George Mimba introubleshooting KLT equipment	1 day	Fri 7/9/99	Fri 7/9/99
48		Perform a weekly technicalsession with Mr. George Mimba	1 day	Fri 7/9/99	Fri 7/9/99
49		Maintained Telemedicine sessions	22 days	Mon 8/2/99	Tue 8/31/99
50		Coordinating Telemedicine taining American Medical Development Inc.	22 days	Mon 8/2/99	Tue 8/31/99
51		Prepare training class	22 days	Mon 8/2/99	Tue 8/31/99
52		Maintained a weekly communication with technical point of contact in Nairobi	23 days	Wed 9/1/99	Thu 9/30/99
53		Coordinate Telemedicine trainig at KLT Telecom Inc. facilities	23 days	Wed 9/1/99	Thu 9/30/99
54		Coordinate refresher training program for the two nurses from Nairobi	15 days	Mon 10/11/99	Fri 10/29/99
55		Completed travel arrangement and training schedule for the two nurses	21 days	Fri 10/1/99	Fri 10/29/99
56		Coordinating remote learning anddemonstrations with AMD representative	21 days	Fri 10/1/99	Fri 10/29/99
57		Coordinating trainee trip, travel expenses and accommodation	21 days	Fri 10/1/99	Fri 10/29/99
58		Sending test cases using store-andforward from Nairobi to ISIS Center	22 days	Mon 11/1/99	Tue 11/30/99
59		Assessment of Immediate needs of Teemedicine services	211 days	Fri 7/9/99	Thu 4/27/00
60		Operation: Technical and Engineering Support	195 days	Mon 8/2/99	Thu 4/27/00
61		Create an e-mail account for theTelemedicine system	1 day	Mon 8/2/99	Mon 8/2/99
62		Obtain static IP address in DoSnt	1 day	Mon 8/2/99	Mon 8/2/99
63		Established a secure IP connection over the DoS's OPEN-Net	23 days	Wed 9/1/99	Thu 9/30/99
64		Evaluate potential store-and-forward Telemedicine systems	23 days	Wed 9/1/99	Thu 9/30/99
65		Trouble shooting guide and instruction manual book for George Mimba	21 days	Fri 10/1/99	Fri 10/29/99
66		Provided Nairobi with User Guide and Technical documentation for VIEWSEND	21 days	Tue 2/1/00	Tue 2/29/00
67		Attended a demonstration at KLT Telecom, Inc.	1 day	Tue 3/14/00	Tue 3/14/00
68		Attended a technical training at KLTTelecom, Inc.	1 day	Tue 3/21/00	Tue 3/21/00
69		Configuration of new workstations to adhere to the protocols of OPEN-Net network conf	1 day	Thu 4/27/00	Thu 4/27/00
70		Business Process Practise	1 day	Fri 7/9/99	Fri 7/9/99
71		TBD	1 day	Fri 7/9/99	Fri 7/9/99
72		Standard operating procedures for Telemedicine consulting outside DoS network	104 days	Fri 7/9/99	Tue 11/30/99
73		Establish protocols to transfer X-ray Images from Nairobi to MED	1 day	Fri 7/9/99	Fri 7/9/99
74		Set clinical and policy directions for store-and-forward Telemedicine	22 days	Mon 11/1/99	Tue 11/30/99
75		Telemedicine consultation procedure and clinical point-of-contact	22 days	Mon 11/1/99	Tue 11/30/99
76		Document procedures and policies *	104 days	Wed 12/8/99	Mon 5/1/00
77		Coordinate the logistics of consults	25 days	Wed 1/26/00	Tue 2/29/00
78		Create DoS Pass for access to building and DoS Telemedicine equipment	1 day	Wed 1/26/00	Wed 1/26/00
79		Acquired security pass to DoS building for Mr. Fikre Alemu	21 days	Tue 2/1/00	Tue 2/29/00
80		Engineering, Technical, and Operations Support	212 days	Fri 7/9/99	Fri 4/28/00
81		Inventory communication and computer equipment	42 days	Mon 1/3/00	Tue 2/29/00
82		Created preliminary inventory for MED, Nairobi, and ISIS	21 days	Mon 1/3/00	Mon 1/31/00
83		Updated the preliminary inventory for MED, Nairobi, and ISIS	21 days	Tue 2/1/00	Tue 2/29/00
84		Periodic inventory checks	1 day	Wed 1/5/00	Wed 1/5/00



Project: NairobiTelemedicineProject2
Date: Fri 6/16/00

Task	▨	Progress	▬	Summary	▬
Split	....	Milestone	◆	Rolled Up Task	▨
Rolled Up Split	....	Rolled Up Progress	▬	Project Summary	▬
Rolled Up Milestone	◇	External Tasks	▨		

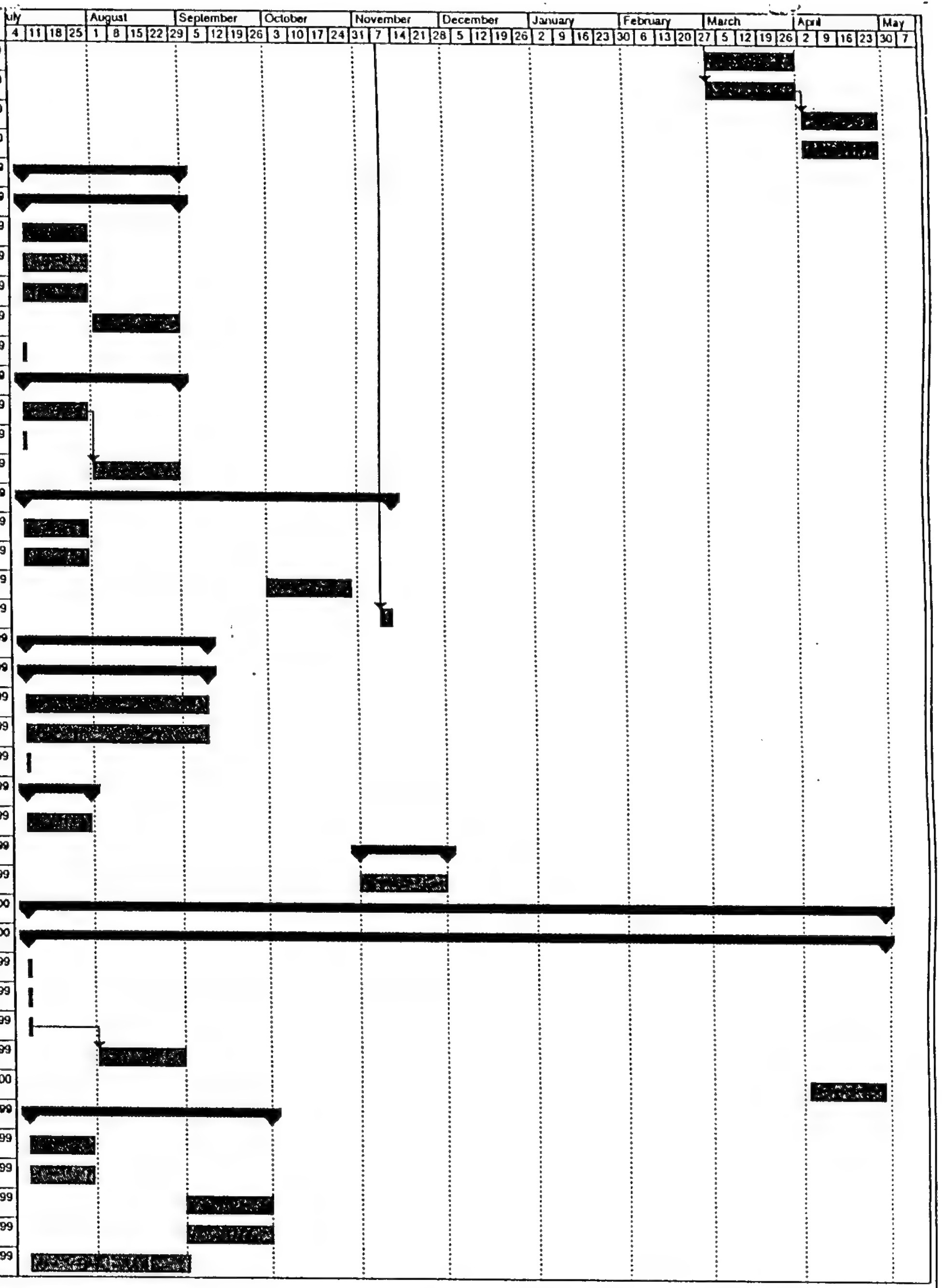
ID		Task Name	Duration	Start	Finish
85		Installation & technical testing	192 days	Fri 7/9/99	Fri 3/31/00
86		Health Unit at Nairobi US Embassy	192 days	Fri 7/9/99	Fri 3/31/00
87		Upgrade MED and Nairobi KLT's VTC equipment software	16 days	Fri 7/9/99	Fri 7/30/99
88		Conducted VTC between Nairobi and ISIS daily to assess the quality of images	16 days	Fri 7/9/99	Fri 7/30/99
89		Supported the relocation of Telemedicine equipment	8 days	Fri 8/20/99	Tue 8/31/99
90		Maintained the system functionality	22 days	Mon 8/2/99	Tue 8/31/99
91		The satellite (VSAT) was moved	1 day	Mon 8/23/99	Mon 8/23/99
92		Forward old video conference spares and equipment to TATRC	1 day	Mon 8/2/99	Mon 8/2/99
93		Accomplished the relocation of the Telemedicine system	23 days	Wed 9/1/99	Thu 9/30/99
94		Created an account with a local Internet Service Provider in Nairobi	23 days	Wed 9/1/99	Thu 9/30/99
95		Resolve all device conflicts and errors	21 days	Fri 10/1/99	Fri 10/29/99
96		Upgraded the SCI board adapter card from 2940 to 2930	21 days	Fri 10/1/99	Fri 10/29/99
97		The upgrade of Nairobi's Telemedicine workstation is complete and the system is fully fu	21 days	Mon 1/3/00	Mon 1/31/00
98		Supplied Nairobi Health Unit with new hard disk	23 days	Wed 3/1/00	Fri 3/31/00
99		Medical Office at DoS	108 days	Fri 10/1/99	Tue 2/29/00
100		Replaced and upgraded the DoS's machine into NT operating system	21 days	Fri 10/1/99	Fri 10/29/99
101		Preparing to move Telemedicine workstation to the clinical exam room	21 days	Mon 1/3/00	Mon 1/31/00
102		Moved MED's Telemedicine Workstation to the clinical examination room	21 days	Tue 2/1/00	Tue 2/29/00
103		Install a network hub at MED	21 days	Tue 2/1/00	Tue 2/29/00
104		Tested the DoS's Telemedicine workstation after the relocation	21 days	Tue 2/1/00	Tue 2/29/00
105		ISIS Center at Georgetown University	66 days	Mon 8/2/99	Fri 10/29/99
106		Tested upgrading a KLT system to a Windows NT Workstation	23 days	Wed 9/1/99	Thu 9/30/99
107		Upgraded three KLT equipment	21 days	Fri 10/1/99	Fri 10/29/99
108		Maintained the system, performing system testing, and have equipment ready	21 days	Fri 10/1/99	Fri 10/29/99
109		Maintained the system functionality	22 days	Mon 8/2/99	Tue 8/31/99
110		Resolve all device conflicts and errors	21 days	Fri 10/1/99	Fri 10/29/99
111		Assess the technical support capabilities	212 days	Fri 7/9/99	Fri 4/28/00
112		Assigned a local engineer to be the technical POC at the Health Unit	16 days	Fri 7/9/99	Fri 7/30/99
113		Train the Nairobi's technical personnel (Mr. George Mimba) at the ISIS Center	20 days	Mon 10/18/99	Fri 11/12/99
114		Performed training session for Mr. George Mimba at the ISIS Center	3 days	Mon 10/18/99	Wed 10/20/99
115		Arranged remote learning and demonstration with AMD representative	3 days	Mon 10/18/99	Wed 10/20/99
116		Video recorded session of troubleshooting for reference material	3 days	Mon 10/18/99	Wed 10/20/99
117		Prepared and provided a troubleshooting guide and instruction manual book	10 days	Mon 11/1/99	Fri 11/12/99
118		Provided a video recorded session of the videoconferencing held with AMD	4 days	Tue 11/9/99	Fri 11/12/99
119		Provided technical support to George Mimba through email	22 days	Mon 11/1/99	Tue 11/30/99
120		Created email accounts on two machines to be able to exchange patient study	22 days	Mon 11/1/99	Tue 11/30/99
121		Support Mr. Mimba to connect into MED's Telemedicine workstations using IP	21 days	Mon 1/3/00	Mon 1/31/00
122		Assisting sending test patients' studies using IP-method	21 days	Mon 1/3/00	Mon 1/31/00
123		E-mail accounts to be utilized in exchanging patients' records: Nairobi: KLTNRB@state.gov, I	21 days	Mon 1/3/00	Mon 1/31/00
124		Provided Mr. Mimba with Lap-link to expedite the trouble shooting process	21 days	Mon 1/3/00	Mon 1/31/00
125		Provided Mr. Mimba with Technical support to troubleshoot the Zydacron card	21 days	Tue 2/1/00	Tue 2/29/00
126		Contacted Zydacron, Inc. to solve Nairobi's Telemedicine Workstation technical problem	21 days	Tue 2/1/00	Tue 2/29/00



Project: NairobiTelemedicineProject2
Date: Fri 6/16/00

Task	▨	Progress	▬	Summary	▬	Rolled Up Split	....	Rolled Up Progress	▬	Project Summary	▬
Split	....	Milestone	◆	Rolled Up Task	▨	Rolled Up Milestone	◇	External Tasks	▨		

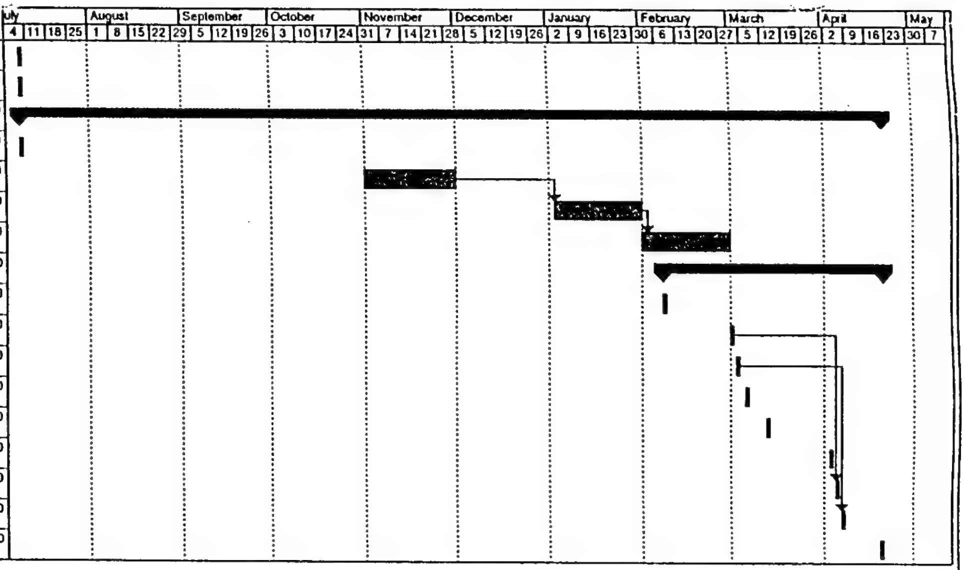
ID		Task Name	Duration	Start	Finish
127		Provided Mr. George Mimba with technical support to solve the X-ray digitizer problem	23 days	Wed 3/1/00	Fri 3/31/00
128		IP Connectivity tests using "ping" command resulted in unsuccessful connection	23 days	Wed 3/1/00	Fri 3/31/00
129		Established IP connection between Nairobi and MED	20 days	Mon 4/3/00	Fri 4/28/00
130		Sent test studies between Nairobi and MED	20 days	Mon 4/3/00	Fri 4/28/00
131		Checks of equipment and communications	38 days	Fri 7/9/99	Tue 8/31/99
132		Equipment in Nairobi	38 days	Fri 7/9/99	Tue 8/31/99
133		Tuned equipment at Nairobi to improve audio and video quality	16 days	Fri 7/9/99	Fri 7/30/99
134		Agreed to conduct a weekly VTC with Nairobi and ISIS/MED every Friday 8 am EST (du	16 days	Fri 7/9/99	Fri 7/30/99
135		Evaluated the opthalmoscope	16 days	Fri 7/9/99	Fri 7/30/99
136		Tested ENT and opthalmoscope brought from Nairobi to troubleshoot	22 days	Mon 8/2/99	Tue 8/31/99
137		Equipment in MED	1 day	Fri 7/9/99	Fri 7/9/99
138		Train clinical personnel in MED Washington and Nairobi Health Unit to use the equipment c	38 days	Fri 7/9/99	Tue 8/31/99
139		Retrained all the nurses in the use of all the peripheral devices	16 days	Fri 7/9/99	Fri 7/30/99
140		Send patient cases (using alias names) from Nairobi to ISIS and MED	1 day	Fri 7/9/99	Fri 7/9/99
141		Simulated Telemedicine sessions	22 days	Mon 8/2/99	Tue 8/31/99
142		Train clinical personnel in MED Washington and Nairobi Health Unit on the clinical capabili	92 days	Fri 7/9/99	Fri 11/12/99
143		Trained clinical personnel at the Health Unit of U.S. Embassy, Nairobi, Kenya	16 days	Fri 7/9/99	Fri 7/30/99
144		Delivered and trained in the use of a versatile dermoscope	16 days	Fri 7/9/99	Fri 7/30/99
145		Store-and-forward test cases will be sent from Nairobi to ISIS Center and MED	21 days	Fri 10/1/99	Fri 10/29/99
146		Provided refresher training sessions for the two nurses practitioners	4 days	Tue 11/9/99	Fri 11/12/99
147		Provide support as necessary in any Telemedicine consult modality that requires technical	46 days	Fri 7/9/99	Thu 9/9/99
148		Technical Support for Nairobi	46 days	Fri 7/9/99	Thu 9/9/99
149		Initiated video conference (while satellite was in use) between Nairobi/ISIS and Nairobi/	46 days	Fri 7/9/99	Thu 9/9/99
150		Initiated video conference (while satellite was in use) between Nairobi/ISIS and Nairobi/	46 days	Fri 7/9/99	Thu 9/9/99
151		Technical Support for MED	1 day	Fri 7/9/99	Fri 7/9/99
152		Act as single point of contact for Telemedicine system problems, communication problem	16 days	Fri 7/9/99	Fri 7/30/99
153		Placed a contact label on the Telemedicine computer for 24-hours technical support	16 days	Fri 7/9/99	Fri 7/30/99
154		Provide access to U.S. clinicians with Telemedicine to provide guidance or support to MED	22 days	Mon 11/1/99	Tue 11/30/99
155		Establish a Telemedicine consultant network within MED	22 days	Mon 11/1/99	Tue 11/30/99
156		Analysis/Evaluation	212 days	Fri 7/9/99	Fri 4/28/00
157		Capture and log Nairobi Telemedicine from start of clinical use	212 days	Fri 7/9/99	Fri 4/28/00
158		Create log of responses to 24-hours technical support when the clinical operation start	1 day	Fri 7/9/99	Fri 7/9/99
159		Create log of the use of the T-Med system when the clinical operation start	1 day	Fri 7/9/99	Fri 7/9/99
160		Publish a web page to log Telemedicine sessions	1 day	Fri 7/9/99	Fri 7/9/99
161		Created a web page to view log of studies	22 days	Mon 8/2/99	Tue 8/31/99
162		Transaction log for test cases sent through email-send and IP-send	20 days	Mon 4/3/00	Fri 4/28/00
163		Problem report and analyze results of problem report	61 days	Fri 7/9/99	Thu 9/30/99
164		On-site technician	16 days	Fri 7/9/99	Fri 7/30/99
165		Installation of an ISDN line	16 days	Fri 7/9/99	Fri 7/30/99
166		Evaluation of the store-and-forward method	23 days	Wed 9/1/99	Thu 9/30/99
167		Telemedicine functionalities will not be pursued further	23 days	Wed 9/1/99	Thu 9/30/99
168		Analyze current use of the system	39 days	Fri 7/9/99	Wed 9/1/99



Project: NairobiTelemedicineProject2
Date: Fri 6/16/00

Task	▨	Progress	▬	Summary	▬	Rolled Up Split	. . . .	Rolled Up Progress	▬	Project Summary
Split	. . . .	Milestone	◆	Rolled Up Task	▨	Rolled Up Milestone ◇		External Tasks	▨	

ID	ⓘ	Task Name	Duration	Start	Finish
169		VTC period when satellite communication was active (July - Sept 1999)	1 day	Fri 7/9/99	Fri 7/9/99
170		Store and Forward period when using OPEN-Net connectivity	1 day	Fri 7/9/99	Fri 7/9/99
171		Recommendation on future use of Telemedicine	206 days	Fri 7/9/99	Thu 4/20/00
172		Review/Support/coordinate the Telemedicine consultation between the Health Unit, Nairobi a	1 day	Fri 7/9/99	Fri 7/9/99
173		Preliminary evaluation of low cost store-and-forward Telemedicine equipment	22 days	Mon 11/1/99	Tue 11/30/99
174		Evaluation of VIEWSEND Medical RIX (Store-and-Forward Telemedicine System)	21 days	Mon 1/3/00	Mon 1/31/00
175		Evaluation of VIEWSEND Medical Model 700 Telemedicine Application	21 days	Tue 2/1/00	Tue 2/29/00
176		Preparation for Pathfinder were undertaken in terms of	53 days	Tue 2/8/00	Thu 4/20/00
177		Dr. Seong K. Min presented to Dr. Dumont and Ms. J. Grise the project plans	1 day	Tue 2/8/00	Tue 2/8/00
178		Prepare to purchase and test 5 KLT Telemedicine workstations	1 day	Wed 3/1/00	Wed 3/1/00
179		Define dates for shipment, installation, testing and training at Telemedicine sites	1 day	Fri 3/3/00	Fri 3/3/00
180		Gathering point of contact information at 5 potential health units	1 day	Mon 3/6/00	Mon 3/6/00
181		Attended CME classes organized by MED Washington for clinical practioners	1 day	Mon 3/13/00	Mon 3/13/00
182		Naming convention for the new Telemedicine computers	1 day	Mon 4/3/00	Mon 4/3/00
183		Ordered 5 new KLT Telemedicine workstations for Project Pathfinder	1 day	Wed 4/5/00	Wed 4/5/00
184		Defined dates for shipment, installation, testing and training at Telemedicine sites	1 day	Fri 4/7/00	Fri 4/7/00
185		Project planning meeting for the Pathfinder Project	1 day	Thu 4/20/00	Thu 4/20/00



Project: NairobiTelemedicineProject2 Date: Fri 6/16/00	Task	▆	Progress	▬	Summary	▬	Rolled Up Split	....	Rolled Up Progress	▬	Project Summary
	Split	....	Milestone	◆	Rolled Up Task	▆	Rolled Up Milestone	◇	External Tasks	▨	

Appendix D: Supporting Document for Previous Technical Reports

May 10, 2000

MEMORANDUM

TO: Dr. Duk-Woo Ro

FROM: Maru Corrada

RE: Request for Further Information for Work Accomplished 1-31 August, 1999 as reported on Monthly Technical Report dated 5 September, 1999 for contract #S-LMAQ-99-D-0116.

Under the Deliverables section of the aforementioned report, we are unable to access the web page created to view log of of studies that were sent to the database enabling to view a log of telemedicine sessions with all the details about the usage. The URL in the report is:
http://www.telemedicine.georgetown.edu/telemedicinelog/telemedicinereport.asp

May 11, 2000

To: Maru Corrada, Suzanne Mason

From: Duk-Woo Ro, Ph.D.

RE: Response to the Memorandum (below) on access to the web page created to view the log of studies that were sent to the database.

Recently, the web server were updated and during the process inadvertently the pointer to the database where the transaction logs resides lost it's link to the URL http://www.telemedicine.georgetown.edu/telemedicinelog/telemedicinereport.asp.

We have fixed the problem and the currently the web page is up and running. We have attached a copy of the printout from the current log page for your reference. Thank you.

- May 10, 2000

- MEMORANDUM

- TO: Dr. Duk-Woo Ro

- FROM: Maru Corrada

- **RE: Request for Further Information for Work Accomplished 1-31 August, 1999 as reported on Monthly Technical Report dated 5 September, 1999 for contract #S-LMAQ-99-D-0116.**

- Under the Deliverables section of the aforementioned report, we are unable to access the web page created to view log of of studies that were sent to the database enabling to view a log of telemedicine sessions with all the details about the usage. The URL in the report is: http://www.telemedicine.georgetown.edu/telemedicinelog/telemedicinereport.asp

May 10, 2000

MEMORANDUM

TO: Dr. Duk-Woo Ro

FROM: Maru Corrada

RE: Request for Further Information for Work Accomplished 1-30 September, 1999 as reported on Monthly Technical Report dated 5 October, 1999 for contract #S-LMAQ-99-D-0116.

Under the Work Accomplished section for Management and Engineering Support of the aforementioned report, we are requesting the account information for the Africa OnLine account established so that the KLT platform has access to the Internet.

Under the Work Accomplished section for Management and Engineering Support of the aforementioned report, please describe in more detail the activities involved in "maintained the system functionality".

Under the Deliverables section of the aforementioned report, please provide the static IP addresses to the KLT system over the DoS OPEN-NET and the contact information for the person responsible for maintaining this IP address.

RE: Request for Further Information for Work Accomplished 1-30 September, 1999 as reported on Monthly Technical Report dated 5 October, 1999 for contract #S-LMAQ-D-0116

Under the Work Accomplished Section for Management and Engineering Support of the aforementioned report, we are requesting the account information for the Africa OnLine account established so that the KLT platform has access to the Internet.

ISP	: Africa Online
Account Name	: MEDNAI
Domain	: africaonline.co.ke
Class	: Unlimited email and Internet
Address	: mednai@africaonline.co.ke
Connection Speed	: Up to 56K
Subscription Period	: One year and three months
Monthly Subscription	: 150 US Dollars (approximately)

Note: This account was set up at the request of the personnel at the Health Unit of Nairobi's US Embassy to access the internet. The project did not fund the subscription cost. Due to the availability of internet access through this account the telemedicine project had the option of sending cases as part of email attachment. However, due to the unreliable nature of the ISP connection (most probably unstable phone line to maintain 56K) no patient cases were sent through this internet account. Internet access is no longer an option for the project since telemedicine transaction will be carried out strictly within DoS OPEN-Net.

Under the Work Accomplished section for Management and Engineering Support of the aforementioned report, please describe in more details the activities involved in "maintained the system functionality".

Because of many unexpected errors and conflicts, we have to always check the workstation and maintain the proper functionality of all the equipments. Especially when we are holding a training session, we have to setup different workstation at different location and assured the proper functionality of all workstation. Details of maintaining the proper functionality of the workstations involve:

1. Setting up different workstations in different location
2. Demo of View Send Application
3. Resolving unexpected errors and conflicts if any
4. .Create a study using Film Digitizer, AMD Scope, and Camera,
5. View an existing and newly created studies
6. Check the configuration and calibration of the VIDAR scanner and the Camera. (For VTC)
7. Share, collaborate, and exchange studies between different workstation
8. Send studies using ISDN, Email, and IP connection

9. Check the proper functionality of all the hardware component of the workstation

Under the Deliverables section of the aforementioned report, please provide the static IP addresses to the KLT system over the DoS OPEN-NET and the contact information for the person responsible for maintaining this IP address.

The static IP addresses for the Telemedicine Workstations over the DoS OPEN-NET are:

MED Center Workstation	: 199.2.206.247
Nairobi Health Unit Workstation	: 10.134.192.24

The person responsible for maintaining Nairobi Health Unit Workstation static IP is MR. George Mimba. Contact Information:

Mr. George Mimba
E-mail: mimbagm@state.gov
Phone: (254) 253-7800 ext. 3137

The person responsible for maintaining MED Center Workstation static IP is MR. John Miller. Contact Information:

Mr. John Miller
E-mail: millerjb2@state.gov
Phone: (703) 898-7813

May 10, 2000

MEMORANDUM

TO: Dr. Duk-Woo Ro

FROM: Maru Corrada

RE: Request for Further Information for Work Accomplished 1-30 October, 1999 as reported on Monthly Technical Report dated 5 November, 1999 for contract #S-LMAQ-99-D-0116.

Under the Work Accomplished section for Management and Engineering Support of the aforementioned report, please provide a brief explanation of what the difference between the comply with the Department of State's network security measures, we have tested and upgraded a KLT system to NT Workstation (Version 4.0 Operating System) reported in October and the closely similar work reported in September.

Under the Deliverables section of the aforementioned report, please provide a copy of the troubleshooting guide and instruction manual book for George Mimba during his training visit at ISIS.

Under the Deliverables section of the aforementioned report, please provide a copy of the video recorded session of troubleshooting techniques for the image capture devices through remote learning and live demonstration via videoconference with AMD provided to George Mimba.

RE: Request for Further Information for Work Accomplished 1-30 October, 1999 as reported on Monthly Technical Report dated 5 November, 1999 for contract #S-LMAQ-D-0116

Under the Work Accomplished Section for Management and Engineering Support of the aforementioned report, please provide a brief explanation of what the difference between the comply with the Department of States's network security measures, we have tested and upgraded a KLT system to NT Workstation (Version 4.0 Operating System) reported in October and the closely similar work reported in September.

According to DoS Security guidelines any PC to be put on the OPEN-NET it has to be running Microsoft Windows NT 4.0 Workstation Operating System. To comply with these guidelines three Telemedicine Workstations have been upgraded from Windows 95 to Windows NT 4.0 at ISIS Center during the month of September in preparation to upgrade MED Center and Nairobi Health Unit workstations. The upgraded machines went through a thorough testing to make sure that the VISWSEND MEDICAL is fully functional when operating uder Windows NT 4.0 Workstation operating system before the equipment at MED was upgraded. During the month of October Mr. Fikre Alemu upgraded MED's workstations into Windows NT 4.0 Workstation and also trained Mr. George Mimba at Georgetown University's ISIS Center to upgrade Nairobi's workstations when he returns to Nairobi, Kenya.

Under the Deliverables section of the aforementioned report, please provide a copy of the troubleshooting guide and instructions manual book for George Mimba during his training visit at ISIS.

From: George Mimba [mailto:mimbagm@hotmail.com]
Sent: Thursday, May 18, 2000 9:12 AM
To: khanafel@isis.imac.georgetown.edu; mimbagm@hotmail.com; mimbagm@state.gov
Cc: ro@isis.imac.georgetown.edu; Alemu@isis.imac.georgetown.edu
Subject: RE: Telemedicine

Hi Labib,

1. The internet account we had on the local ISP was MEDNAI.

2. The IP Address we had on the NRB-RMO-KLT-01 Telemedicine system was 10.134.192.24 and the DOS Ip we were connecting to was 199.2.206.247. We were sending test cases using IP connect. However this could still be done using the computer name.

3. I have asked Trusha and Barbara to send you an email confirming they brought with them video tape and the manual.

4. I had confirmed that I came to ISIS last year in Spring and had technical training both at KLT and ISIS. I also attended a DEMO by AMD on the Scope which I brought to Nairobi and installed. I was given a Video of the DEMO as well manual and Troubleshooting tips. I also received a screen capture of the common problems and how one goes around solving them. This I received from Fikre!

I also received an updated Viewsend manual from you (Labib). All these documentations are well kept in the telemedicine room.

I hope this answers your questions. Feel free to contact me if you need any additional info. George.

Under the Deliverables section of the aforementioned report, please provide a copy of the video recorded session of troubleshooting techniques for the image capture devices through remote learning and live demonstration via videoconference with AMD provided to George Mimba.

From: George Mimba [mailto:mimbagm@hotmail.com]
Sent: Thursday, May 18, 2000 9:12 AM
To: khanafel@isis.imac.georgetown.edu; mimbagm@hotmail.com; mimbagm@state.gov
Cc: ro@isis.imac.georgetown.edu; Alemu@isis.imac.georgetown.edu
Subject: RE: Telemedicine

Hi Labib,

1. The internet account we had on the local ISP was MEDNAI.

2. The IP Address we had on the NRB-RMO-KLT-01 Telemedicine system was 10.134.192.24 and the DOS Ip we were connecting to was 199.2.206.247. We were sending test cases using IP connect. However this could still be done using the computer name.

3. I have asked Trusha and Barbara to send you an email confirming they brought with them video tape and the manual.

4. I had confirmed that I came to ISIS last year in Spring and had technical training both at KLT and ISIS. I also attended a DEMO by AMD on the Scope which I brought to Nairobi and installed. I was given a Video of the DEMO as well manual and Troubleshooting tips. I also received a screen capture of the common problems and how one goes around solving them. This I received from Fikre.

I also received an updated Viewsend manual from you (Labib). All these documentations are well kept in the telemedicine room.

I hope this answers your questions. Feel free to contact me if you need any additional info. George.

May 10, 2000

MEMORANDUM

TO: Dr. Duk-Woo Ro

FROM: Maru Corrada

RE: Request for Further Information for Work Accomplished 1-30 November, 1999 as reported on Monthly Technical Report dated 5 December, 1999 for contract #S-LMAQ-99-D-0116.

Under the Deliverables section of the aforementioned report, please provide a copy of the troubleshooting guide and instruction manual book for two nurses during their training visits at ISIS. (If not already provided from the request made on the Monthly Technical Report dated 5 November, 1999.)

Under the Deliverables section of the aforementioned report, please provide a copy of the video recorded session of the videoteleconferencing held with AMD provided to the two nurses. (If not already provided from the request made on the Monthly Technical Report dated 5 November, 1999.)

Under the Deliverables section of the aforementioned report, please provide a clear conclusion to the Technical Product Overview detailed in section 3 of the same report. Please provide the Evaluation Criteria and Product Testing Approaches to be used in the ongoing evaluation effort that is planned.

June 13, 2000

To: Maru Corrada, Suzanne Mason

From: Duk-Woo Ro, Ph.D.

RE: Request for Further Information for Work Accomplished 1-30 November, 1999 as reported on Monthly Technical Report dated 5 December, 1999 for contract #S-LMAQ-D-0116

Under the Deliverables section of the aforementioned report, please provide a copy of the troubleshooting guide and instructions manual book for two nurses during their training visits at ISIS. (If not already provided from the request made on the Monthly Technical Report dated 5 November, 1999.)

From: Muli, Barbara E [mailto:MuliBE@state.gov]
Sent: Monday, May 22, 2000 1:29 AM
To: 'labib'
Subject: Requested Info.

Good morning Labib, I notice you never write to us anymore. We are feeling a little left out. Anyway, how are you? Pass my regards to everyone. George tells me that we will be able to start transmiting soon. I hope it works. Now, we did get the tape and the folder that you made for us,during the training. That is all we have. Was there something else that you gave us?
Barb

Under the Deliverables section of the aforementioned report, please provide a copy of the video recorded session of the videoteleconferencing held with AMD provided to the two nurses. (If not already provided from the request made on the Monthly Technical Report dated 5 November, 1999.)

From: Muli, Barbara E [mailto:MuliBE@state.gov]
Sent: Monday, May 22, 2000 1:29 AM
To: 'labib'
Subject: Requested Info.

Good morning Labib, I notice you never write to us anymore. We are feeling a little left out. Anyway, how are you? Pass my regards to everyone. George tells me that we will be able to start transmiting soon. I hope it works. Now, we did get the tape and the folder that you made for us,during the

training. That is all we have.Was there something else that you gave us?
Barb

Under the Deliverables section of the aforementioned report, please provide a clear conclusion to the Technical Product Overview detailed in section 3 of the same report. Please provide the Evaluation Criteria and Product Testing Approaches to be used in the ongoing evaluation effort that is planned.

The following list is the evaluation criteria which are used to evaluate the different Telemedicine Systems:

1. What Operating Systems does the application support, such as:
   a. Windows 95
   b. Windows NT Workstation
   c. LINUX
   d. etc.
2. What Methods does the application use to Tele-:
   a. IP
   b. E-mail
   c. FTP
   d. etc.
3. Does the application support Internet
4. Security (i.e. medical data encryption, e-mail encryption)
5. Patient Record Management
6. Does the application support videoconferencing and what network methodology does it use to videoconference (i.e. IP, ISDN, etc.)
7. Multimedia capture
   a. TWAIN compliant
   b. DICOM images (i.e. X-ray, MRI, CT)
   c. Scanned photos
   d. Digital camera
   e. Capture still and live video

   f. Capture audio clips

8. Image
   a. Annotation (e.g. text, lines, circles, boxes, etc.)
   b. Manipulating (e.g. pan, zoom, rotate, etc.)
   c. Collaboration
9. Image printing
10. Image compression
11. The ability to interface with different peripherals, such as:
    a. Film digitizers
    b. Medical scopes (i.e. ENT, Dermascopes, etc.)
    c. Capture cameras
    d. Digital cameras
    e. Scanners
12. Client/Server Architecture

According to the above criteria the qualified Telemedicine systems are:

- STAT from Aethra
- MedVizer from ViTel Net
- VIEWSEND from KLT Telecom, Inc.

The advantages of VIEWSEND over the other two systems are:

- The experience of ISIS Center technical staffs' with VIEWSEND Medical which will ease the learning curve and the technical support of the new sites.
- The ability of to custom design VIEWSEND features according to DoS and ISIS Center needs (i.e. Security guidelines).
- The experience and familiarity of Nairobi Health Unit's nurses and technical personnel with the previous version of VIEWSEND Medical.

- Because of the experience Nairobi Health Unit have with VIEWSEND Medical that will help in supporting the new African sites through them.

The product evaluation is carried out by reviewing product specification available on manufacturer's web page and product catalogs. Telephone inquires of the system and their functionalities are also made.

May 10, 2000

MEMORANDUM

TO: Dr. Duk-Woo Ro

FROM: Maru Corrada

RE: Request for Further Information for Work Accomplished 1-30 November, 1999 as reported on Monthly Technical Report dated 5 December, 1999 for contract #S-LMAQ-99-D-0116.

Under the Deliverables section of the aforementioned report, please provide a copy of the troubleshooting guide and instruction manual book for two nurses during their training visits at ISIS. (If not already provided from the request made on the Monthly Technical Report dated 5 November, 1999.)

Under the Deliverables section of the aforementioned report, please provide a copy of the video recorded session of the videoteleconferencing held with AMD provided to the two nurses. (If not already provided from the request made on the Monthly Technical Report dated 5 November, 1999.)

Under the Deliverables section of the aforementioned report, please provide a clear conclusion to the Technical Product Overview detailed in section 3 of the same report. Please provide the Evaluation Criteria and Product Testing Approaches to be used in the ongoing evaluation effort that is planned.

Appendix E: Technical Documents for the Pathfinder Project

U.S. Department of State
Office of Medical Services
M/DGP/MED

"Pathfinder" – Joint DoD & Georgetown University Medical Center Telemedicine Pilot project participation by M/DGP/MED

Project introduction meeting – 3 May 2000
Meeting notes

Attendees:
Kim Johnson IRM/OPS/ITI/SI
Tin Cao IRM/OPS/ITI/SI
Jean Garneau IRM/OPS/ENM/NED
Linda Safta IRM/CST/LD/DB
Carey Moore IRM/CST/LD/DB
Randy Nash DS/SAB
Jennifer Grise MED/EX/INF
Curtis Barefield MED/EX/INF/SYS
Labib Khanafer Georgetown University Medical Center ISIS
Fikre Alemu Georgetown University Medical Center ISIS

Summary of project -

- DoD & Georgetown University funded, planned, and supported project, which can only be supported through December 2000.
- Department of State is invited to play a role as a pilot participant.
- MED Management would like to participate in order to answer some basic study questions for the Department. This is part of MED's planning in order to provide quality health care services to Foreign Affairs agencies in an environment of increasing risks to health and safety.

Medical Program study questions -

1. Can a telemedicine services platform operate effectively within the Department of State's unclassified network?

2. Will a telemedicine services platform make a difference in the quality of patient care services in the Department's Medical Program?

Overview of proposed pilot –

- CONUS sites would be – MED Washington, Regional Medevac Center, Ft Lauderdale
- Overseas sites proposed are – Nairobi, Dar es Salaam, Kampala, Port au Prince, Santo Domingo
- Store and forward technology, would be used (real-time transactions are not manditory requirement of pilot). Email could be used to transmit.
- Files could be – digitized X-rays, digital photos, whiteboard transmissions, scanned documents
- Cases could be coded with numbers, instead of revealing patient identifiers

Unanswered questions at this meeting –

- Specifics of the client/server architecture
- Type of connections necessary – "session to session"?, other?
- Sample sizes of files
- Specifications of COTS software to be used for the transactions
- Encryption strategies, if any, for system

Possible obstacles to starting proposed pilot –

- Poor post choice(s), from a technical point of view
- Network load issues, overall
- Appropriateness of software application/platform

Suggested next steps –

1. MED to send one page project summary to IRM/OPS/ENM (Enterprise Network Management) together with a request that ENM initiate a project to support this effort with MED. Effort would include, at a minimum, working together with MED to develop a grid of posts where such a telemedicine platform would be technically feasible. This effort could also include live testing in a simulated overseas environment, in ENM lab here in Washington.
2. MED to consider again, whether it may be worthwhile to seek DS approval of using an internet platform for such a pilot. It is doubtful, due to issues of medical confidentiality, and the short time window of opportunity to participate in this project.
3. MED to provide detailed documentation to DS/SAB on the software systems proposed for the pilot, for review in advance of CCB review.
4. MED to seek CCB approval for such a pilot, providing detailed documentation as requested. This documentation would need to include (but not be limited to) technical architecture, project plans, specifications. Approval time after submission of all documentation would be at least 3 weeks – could be more.

Georgetown University
ISIS Center
May 2000

Technical responses to unanswered questions at the meeting on 5/3/2000

- Specifics of the client/server architecture

Response: The telemedicine platform, currently installed in Nairobi and MED Washington, VIEWSEND™ Medical is not a client/server system. Image transfer, annotation and collaboration are on a peer to peer basis.
If current project requires the need for a client/server system the KLT, Inc. that developed the VIEWSEND™ Medical has designs for a client/server architecture that is available from one of their OEMs.

- Type of connections necessary – "session to session"?, other?

Response: Connection type is based on available bandwidth at the post. Complete study information may be transmitted via email. When opened, the email meshes seamlessly with the recipient's database. Email takes advantage of least cost routing to OpenNet locations and off-net locations. Connections may be resolved using DHCP and a name server or static IP Addresses. Audio connections are available with as little as 16kbps of bandwidth. Minimum data channel for collaboration is 6kbps. Minimum channel to support Video/Audio/Data is 64kbps. File transfer via FTP takes advantage of whatever bandwidth is available.

- Sample sizes of files

Response: The size of a study is directly proportionate to the complexity of the content and the level of compression used in saving the file. A typical full chest x-ray digitized at 150DPI and 12-bit depth may easily require 1.8MB of storage. With only modest compression, the image can be stored and transmitted using 900kb of space or less.
Wavelet compression may provide as much as 30 to 1 compression.
JPEG Lossless compression is considered to be 2 to 1.
JPEG Lossy compression is user adjustable with unacceptable degradation occurring at about 12 or 16:1.

Other typical image sizes:

Single frame MRI – 300kb
Small x-ray (e.g. hand) 35kb
JPEG dermascopic (or other video) image – 3kb
Study demographics – 3k
Recorded voice annotation 8kb per second recorded.

Low Speed Transfer Times (in seconds)

Rate(Kbps)						
I			FILE SIZE			
I	40Kb	50Kb	100Kb	200Kb	500Kb	1000Kb
14.4	35.79	43.98	84.97	166.93	412.84	822.67
19.2	26.53	32.41	61.82	120.65	297.12	591.24
21.6	23.62	28.77	54.55	106.09	260.73	518.46
28.8	18.04	21.80	40.59	78.19	190.97	378.94

	LEGEND
Kbps	Kilo-bits per second
Kb	Kilo-bytes

➢ Specifications of COTS software to be used for the transactions

Software that has a direct bearing on the operation of VIEWSEND Medical:

1. Data Access Objects Version 3.50
2. VCON MeetingPoint SDK distribution version 4.01
3. Microsoft Netmeeting 2.1(4.3.2203)
4. Microsoft Internet Explorer Ver 4.X
5. VIEWSEND™ Medical Version 7.0.162
6. EZ-SCSI 5.0
7. TWAIN for VIDAR Scanner 4.23
8. Users choice of email software that is MAPI compliant.
9. Windows NT 4.0 Workstation with Service Pack 4

➢ Encryption strategies, if any, for system

The encryption strategy for VIEWSEND Medical systems is based on the standard Public-Key/Symmetric-Key encryption methodology. As an example of a store and forward transmission using email, all patient information and medical imaging are packaged, compressed, and then encrypted with a private 128-bit key. This private is used at the receiving site to decrypt and retrieve the patient medical data. In addition, KLT offers the following encryption package in collaboration with VCON.

KLT and VCON provides option for TopSecret IP^{TM} - the new encryption add-on software for all KLT AND VCON's IP-based products. TopSecret IP^{TM} provides high quality security against both unauthorized participation and eavesdropping during videoconferences over your IP networks.
TopSecret IPTM is an easy to use software add-on that protects a videoconference's transmissions in real-time, without affecting the Quality of Service (QoS). The new encryption module will be sold as an optional add-on, designed especially for IP networks.

The module represents an industry first and is expected to meet the needs of those organizations and enterprises which are increasingly turning to videoconferencing as an everyday tool to conduct business, but which require guaranteed confidentiality or secrecy due to the sensitive nature of the information being communicated during sessions.

TopSecret IPTM supports both point-to-point and interactive multicast conferences and consists of a choice of three real-time encryption/decryption algorithms, each of which is effective in securing video, audio and broadband file transfers. They are all based on the Diffe-Hellmann private/public key mechanism considered by security experts to be ultra-effective against penetration. The three encryption algorithms are as follows:

CipherActive: The TopSecret IPTM encryption algorithm, consisting of real-time, high level security, encryption/decryption software code. Its software acceleration engine significantly speeds up the encryption process of standard algorithms.

DES Data Encryption Standard - a symmetric encryption security type. The same key is used by both sender and receiver. The sender's message is encrypted using one algorithm, based on a 56-bit key length. The receiver deciphers the message using the algorithm and key in reverse order.

IDEA^{TM} International Data Encryption Algorithm - a new, universally applicable block encryption algorithm, with a 64-bit block length and a 128-bit key. It permits the effective protection of transmitted and stored data against unauthorized access by third parties.

From: Grise, Jennifer L [GriseJL@state.gov]
Sent: Friday, May 12, 2000 9:28 AM
To: 'Mun, Seong Ke (G'tn ISIS)'; 'Ro, Duk Wo (G'tn ISIS)'; Herbert, Dion L
Cc: Weber, Guy A; Corrada, Maru E
Subject: Today's "Pathfinder" telemedicine meeting

Importance: High

I look forward to seeing you all at today's "Pathfinder" Telemedicine Pilot project meeting.
1 pm to 2:30 pm, Office of Medical Services, 2401 E St, NW, Columbia Plaza Office Building

Someone from my office will meet you in the lobby a few minutes before 1 pm, to direct you to the conference room.
(If you arrive later, just check in with the guard. The guard can call x31611 or x31649 to get clearance for you.
You can then proceed to Rm. L-209, and ask to be directed to the Medical Director's conference room.)

The meeting objectives for today are to:

1. Finalize roles and who will fill them on this project

2. Review suggested project schedule

3. Define what constraints there are, on proceeding with project

4. Determine how we can achieve our objectives with those constraints, or can remove constraints

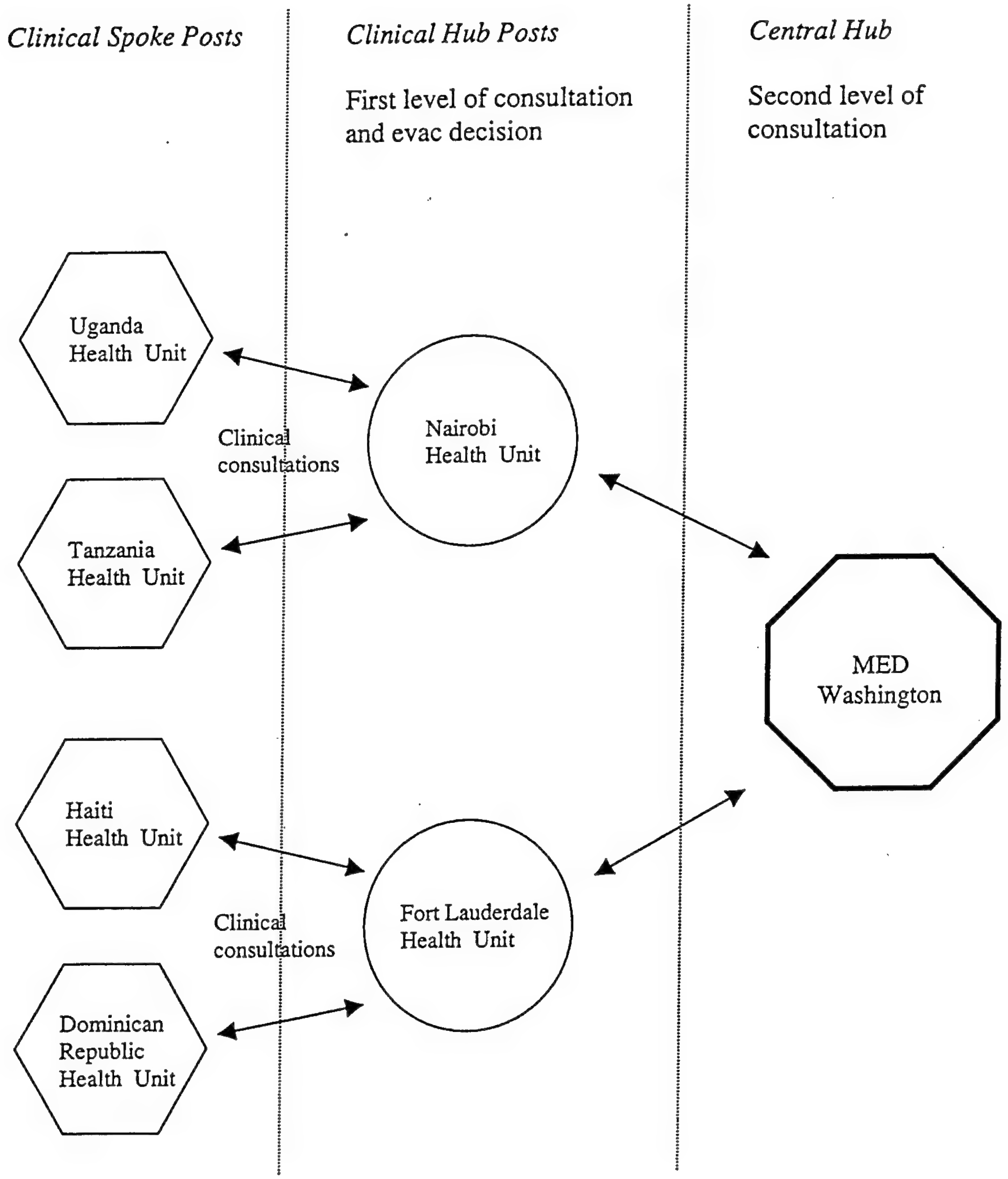
Meeting agenda:

1. Discussion of objectives above
2. Status update on:

* Operations description document & basic suggested project schedule - from Georgetown
* MOA document draft
* Finding posts that are acceptable to all parties
* Technical documentation necessary for State Configuration Control Board (CCB) consideration for approval

- Jennifer Grise
Division Chief, Medical Informatics
MED/EX/INF
U.S. Department of State
202.663.1690

Clinical Operation Flow



Georgetown University
ISIS Center
5/12/2000

Tentative Project Schedule – Project Pathfinder

30 May, 2000	Complete installation in Kenya, Uganda**, Tanzania** and MED KLT workstation Film Digitizer Document Scanner (**Confirmation needed as approved site for deployment). * Refurbish current KLT workstations at MED and Nairobi
10 June, 2000	Complete training of clinical practitioners in African Posts
1 July, 2000	Start trial period in the use of telemedicine system at African Posts
28 July, 2000	Complete installation in Port-au-Prince, Santo Domingo and Fort Lauderdale
22 September, 2000	Network System demonstration for management
30 November, 2000	Patient Care demonstration

Department of State
Office of Medical Services
Medical Informatics Division

Telemedicine Pathfinder Project
Project Summary – 8 May 2000

Background

The Department of State has many diplomatic missions located in places where good health care is impossible to obtain. Clinical programs must be planned that will allow the Department to provide increased quality health care services to Foreign Affairs agencies in an environment of increasing risks to health and safety. The Office of Medical Services is exploring the potential use of telemedicine services to improve the quality of health care delivered by the Department to those difficult-to-serve-locations.

The Department of Defense has selected the Department of State as one of 3 participants in the piloting of telemedicine services, through December 2000, in U.S. Government agency health care programs. "Pathfinder" is a proof-of-concept project funded, planned and supported by the Department of Defense, and staffed largely by Georgetown University Medical Center's Imaging Science & Information Systems Center (ISIS). Georgetown's ISIS Center has a cooperative agreement with DoD (DAMD 17-94-V-4015) to act as the research partner in this work. This pilot project will provide the Office of Medical Services with valuable information necessary to determine whether deploying telemedicine will enhance the Department's Medical Program.

Telemedicine applications may function to reduce direct and indirect costs of patient care and improve the quality of organizational and customer service. These applications can address specific clinical, medical-education and medical program administrative needs. The Pathfinder pilot project is designed to establish a robust technical foundation from which the uses of telemedicine services can be explored.

Objectives

- Determine whether a telemedicine services platform operates effectively within the Department of State's unclassified network.
- Show whether a telemedicine services platform will increase the quality of medical services in the Department – patient care, medical education, and program administration.

Overview of proposed pilot project

A clinical model for telemedicine using store-and-forward technology has been selected, with post selection recommended by the Medical Director that includes MED Washington and the Regional Medevac Center in Ft. Lauderdale. Overseas sites proposed are Embassy Health Units in Nairobi, Dar es Salaam, Kampala, Port au Prince, and Santo Domingo. State MED Health care providers at the CONUS sites, and select overseas sites, would provide remote patient care using digitized x-rays, digital photos, whiteboard transmissions and scanned documents within the telemedicine platform. Patient confidentiality would be maintained by avoiding use of individual identifiers. Medical education and program administration transactions would occur between CONUS sites and the overseas sites.
Concurrent with this operational pilot, institutional policies and procedures and methods for secure data management in telemedicine, would be developed by MED.

Department of State
Office of Medical Services

Team Action List
Pathfinder Project

Telemedicine
5/12/2000

PATHFINDER					
Finalize equipment funding.	Grise	MED	4/24	Done	$93,000.00
Finalize roles and who will fill them.	Grise	MED	5/2	Done	Separate document.
Project schedule (clinical milestones only)	Ro	GU	5/12		Separate document.
Suggested language for MOA document	Mun	GU	5/12		
Technical documentation for CCB	Ro/Weber	GU	5/12		
Identify technical lead for the project	Mun	GU	5/12		Dr. Ro.
Document clinical/research objectives.	Grise	MED	5/12	Done	Separate document.
Post re-evaluation with MED Management	Grise	MED			
NAIROBI					
Finalize payment and invoicing on current contract (Nairobi)	Corrada	MED	5/3	Done	In process at GU - Dr. Ro.
Summary document for remaining work on current contract (Nairobi)	Corrada	MED	5/5		In process at GU - Dr. Ro.
Clinical operations diagram for t-med services	Ro	GU	5/12		
Provide equipment specs for workstations & peripherals.	Ro	GU			Pending technical meeting week of 5/8.
Complete equipment purchases by July '00.	Weber	GU			Modification for equipment funds completed 4/24.

Department of State
Office of Medical Services

Schedule Milestones
Pathfinder Project

Telemedicine
5/12/2000

1	end of 5/00	for deploying workstations (HW & SW) to Kampala, Dar es Salaam, and Washington
2	early 6/00	for training in Kampala & Dar
3	late 6/00	for refurbishing 2 workstations (HW & SW)
4	early 7/00	possible fact-finding, proj mgt trip to Port au Prince, Santo Domingo, and Ft. Lauderdale
5	mid 7/00	deploying workstations in Port au Orince, Santo Domingo, and Ft. Lauderdale
6	7/28/00	complete training in Port au Prince, Santo Domingo, and Ft Lauderdale
7	9/22/00	Demonstration of fully operative system (and any use results to date)
8	11/22/00	Patient care demonstration, including clinical caseload results to date
9	12/31/00	Pathfinder pilot ends final results are documented

Department of State
Office of Medical Services

Project Contacts
Pathfinder Project

Telemedicine
5/12/2000

	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Jennifer Grise	Dr. Cedric Dumont		Kim Johnson	Dr. Seong Ke Mun	Mr. Kap Kim
	202-663-1690	Gary Alexander		202-647-1223		
[redacted]	Guy Weber		Dion Herbert (ENM)	Tim Cao (PKI)	Dr. Duk-Woo Ro	
	202-663-1758					
[redacted]	Maru Corrada	Barbara Mahoney			Dr. Duk-Woo Ro	
	202-663-1763					

Information
Resource
Management

Appendix F: Teleconsulting Operation Manual

Teleconsulting Operation Manual for
MED Washington and Health Unit in Nairobi, Kenya

Provided to MED of US State Department as part of deliverables for

Contract Number: S-LMAQM-99-D-0116

"NAIROBI TELEMEDICINE PROJECT"

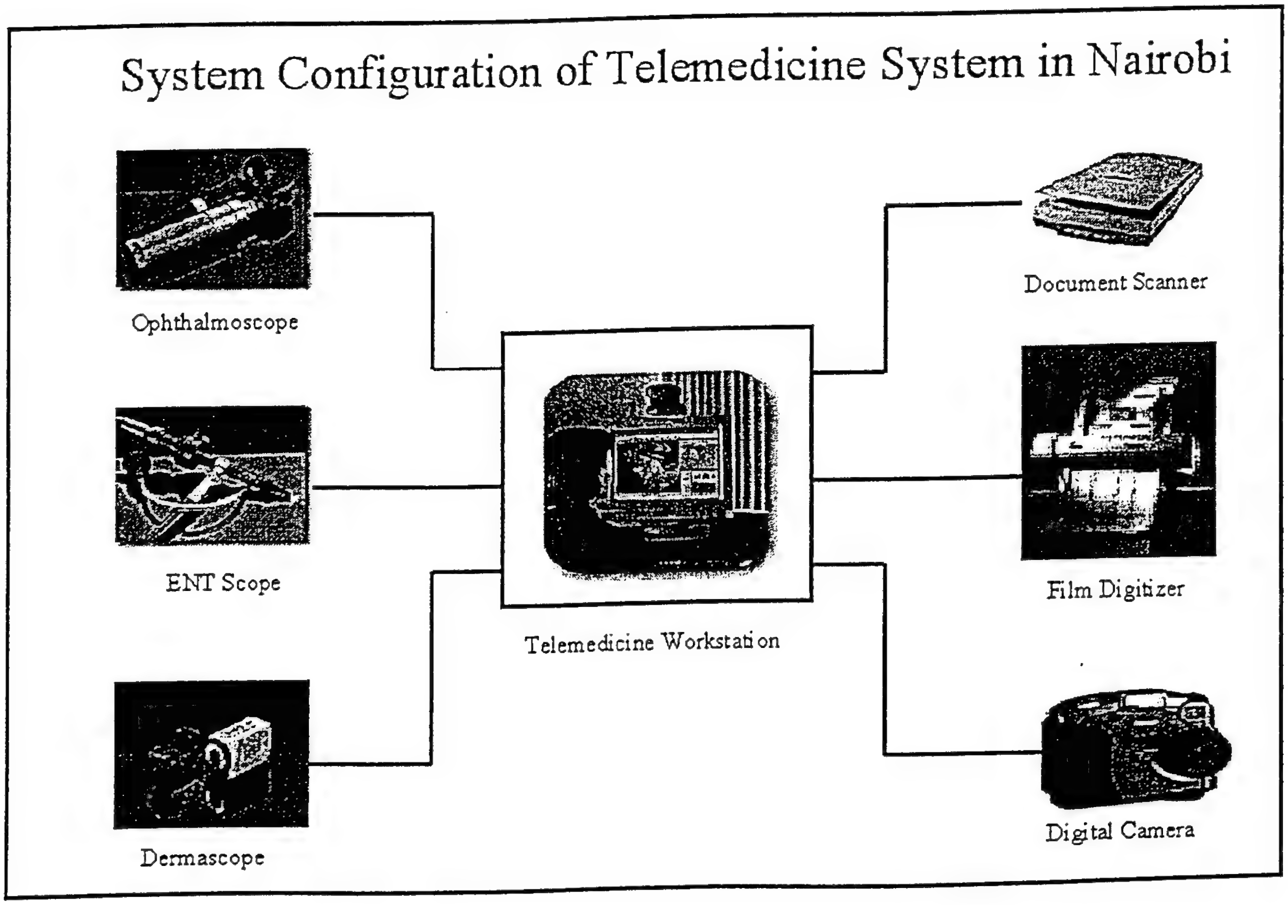
Principal Investigator: Seong K. Mun, Ph.D.
Program Manager: Dukwoo Ro, Ph.D.
ISIS Center, Department of Radiology
Georgetown University Medical Center
Washington, DC 20007
(202) 687-7955

19 May, 2000

Table of Contents

Introduction to MED-Nairobi Teleconsulting Procedures

System diagram of the telemedicine platform installed and in operation at the Health Unit in Nairobi, Kenya, is shown below. The main telemedicine workstation, a PC with MS NT operating system, is connected to various digital input devices and they are; **X-ray film digitizer** to scan films and convert analog signal to digital data, **document scanner** to scan patient charts and clinical data recorded on paper (such as EKG tracings), **digital ophthalmoscope** to capture digital images of patient's eye examination, **digital ENT scope** to capture digital images of patient's nose, ear and mouth examination, **digital dermascope** to capture digital images of general physical examination of patient and patient's skin, **digital camera** to capture video clips and still images of patient's physical examination. In addition, a remote controlled video camera is connected to the Telemedicine Workstation as part of the system and can be used both for video-conferencing between two remote sites and as a general-purpose low-resolution video capture device for patient physical examination. In order to meet the requirements of the State Department's security protocols, the remote controlled video camera has been disabled. The Telemedicine Workstation also includes a speaker and a microphone for teleconferencing, however they both are disabled to meet the security protocols. The unit installed at MED Washington is a similar system with only the Telemedicine Workstation. The two telemedicine workstations are on the OPEN-Net, and both IP transfer and email attachments are used to store-and-forward patient's cases for telemedicine consultation between MED Washington and Nairobi.



Teleconsulting Modules

Teleradiology

Teleradiology is a featured part of the VIEWSEND program. Medical images can be transmitted to an unattended remote site prior to a medical consultation call (and option is available if a modem is installed to the system that a recipient can be paged to notify them of image arrival).

Telemedicine

VIEWSEND is not limited to Radiological information. Images captured by many scopes (ENT, ophthalmoscope, dermascope, etc.) and other devices, for example a flat-bed scanner, can be sent, stored and manipulated by VIEWSEND software.

Patient Study Folders

Images and documents are organized on the PC in patient study folders ideally suited for receiving downloaded images and records from a main archival storage system. While not intended as a long-term storage media for all patient image data, the VIEWSEND system is only limited by the capacity of the storage media available to the PC. A limited amount of textual information is also stored with each study and is entered using a `Study Folder Information' form. A floating, customizable tool palette containing numerous measurement and annotation tools is at the core of VIEWSEND Receive.

Examining Patient Medical Images

Medical images often need more than cursory visual examination. VIEWSEND provides a comprehensive Tool Palette enabling measurement of image cross-sections showing distance, angles, and histograms. Medical images can be magnified, false colored and contrast enhanced to reveal details in the captured image not displayed on the current screen. Notes can be attached to the image for later review. Before and after comparisons of similar medical images can be made to determine the effectiveness of treatment.

Organization of Patient Information

Study

VIEWSEND Medical stores information in a hierarchical fashion starting with a patient study at the top. The Patient Work List contains all studies available on the individual PC where VIEWSEND Medical is installed. The Patient Work List serves as a home base, or starting point for viewing, administering and sending patient images.

A given patient can have any number of studies with each study representing a single treatment instance or a collection of information to be tracked as a single entity. For example, a patient may have any combination of X-ray, CT, MR, ultra-sound, etc. included in one study.

Series

A series is one or more images depending on the originating modality. For example, a series generated by a X-ray machine will have a single image, while a series generated by a DICOM compliant modality, like a MRI, will usually contain multiple images.

Image

This is the smallest element collected and can best be thought of as a "snapshot" or instant in time.

Quick Start Guide in Tele-Consulting Procedures

The following sections provide a quick start guide in the basic steps required to open an existing study, creating a new patient study, taking a snapshot using the onboard frame-grabber, digitizing a film using a digital film digitizer and paper document using a flatbed document scanner and adding that study to an existing patient folder, and sending studies through IP connection as well as email attachments. The instructions on how to use the digital ophthalmoscope, ENT scope and dermascope were videotaped and provided to the nurses stationed at the Health Unit in Nairobi as part of the deliverable for this contract. A more detailed procedures using the tools available on the Viewsend software application are also described in the following chapters. The purpose of this section is to allow users not familiar with all the functions available on the telemedicine application software to perform the basic technical teleconsulting steps in sending and receiving patient exams between MED Washington and the Health Unit in Nairobi, Kenya. To summarize, the following steps will be described using graphical icons and screen captures obtained from the software application to acquaint the users with the graphical user interface (GUI):

- How to open a study
- How to create a new patient study
- How to take a snapshot and add to a study
- How to digitize a film and create or add to a study
- How to scan a document and add to a study
- How to send study through IP
- How to send study through email

How to Open a Study

When you open an existing patient's study, you are able to see all images and notes about the patient.

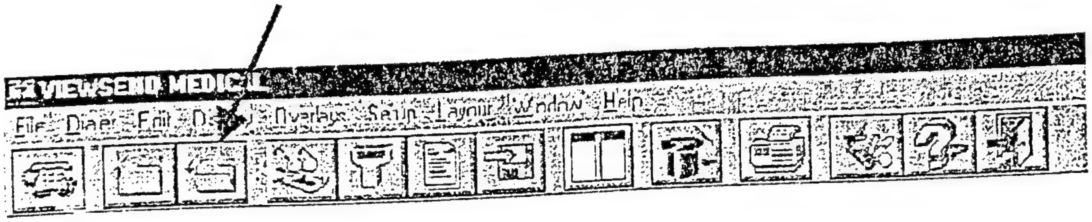
1. Run **VIEWSEND Medical** (double click VIEWSEND Medical icon)

This page left blank intentionally

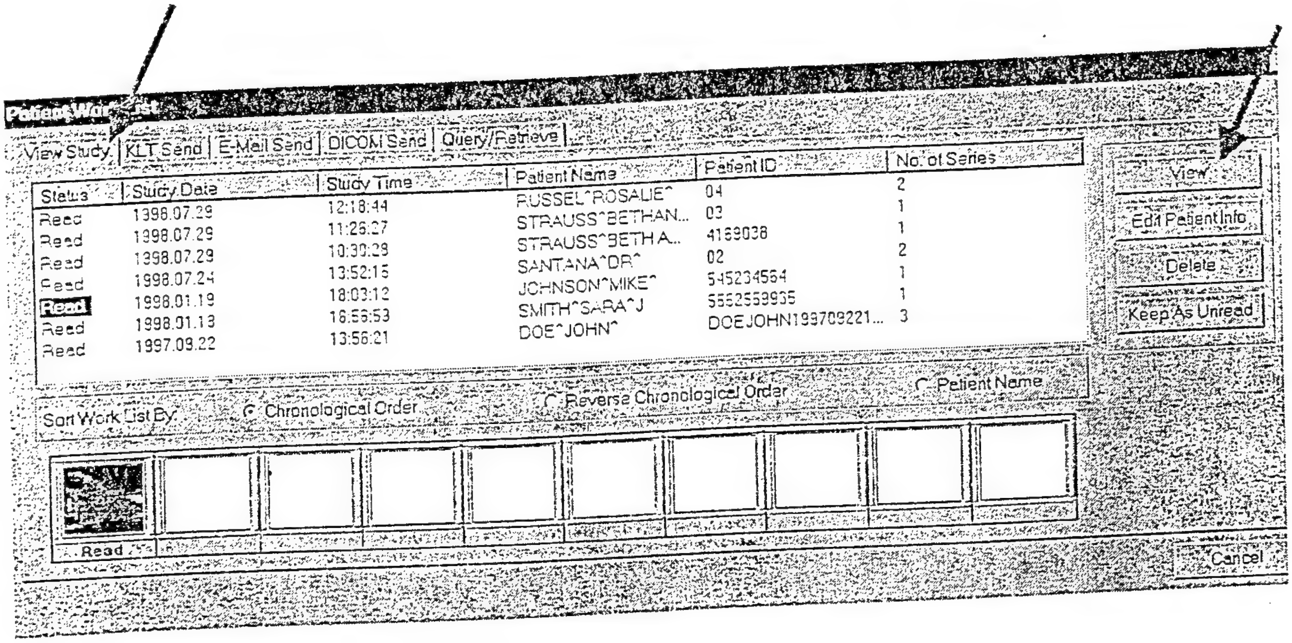
This page left blank intentionally

This page left blank intentionally

2. On the main Toolbar click on the View Patient Work icon.



3. Select View Study tab.



Status	Study Date	Study Time	Patient Name	Patient ID	No. of Series
Read	1998.07.29	12:18:44	RUSSEL^ROSALIE^	04	2
Read	1998.07.29	11:26:27	STRAUSS^BETHAN...	03	1
Read	1998.07.29	10:30:28	STRAUSS^BETH A...	4169038	1
Read	1998.07.24	13:52:15	SANTANA^DR^	02	2
Read	1998.01.19	18:03:12	JOHNSON^MIKE^	545234564	1
Read	1998.01.13	16:56:53	SMITH^SARA^J	5552559935	1
Read	1997.09.22	13:56:21	DOE^JOHN^	DOEJOHN199709221...	3

Sort Work List By: ● Chronological Order ○ Reverse Chronological Order ○ Patient Name

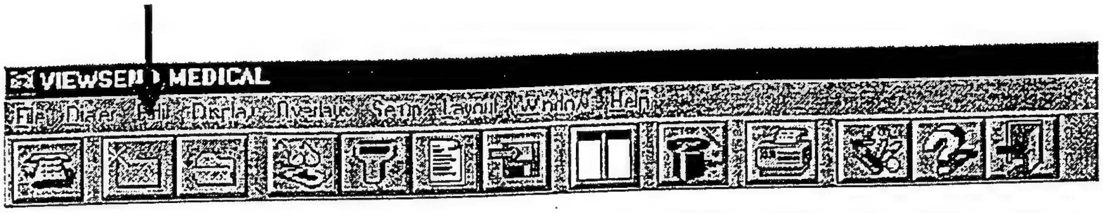
4. Select patient from Patient Work List, click on View.

How to Create a New Patient Study

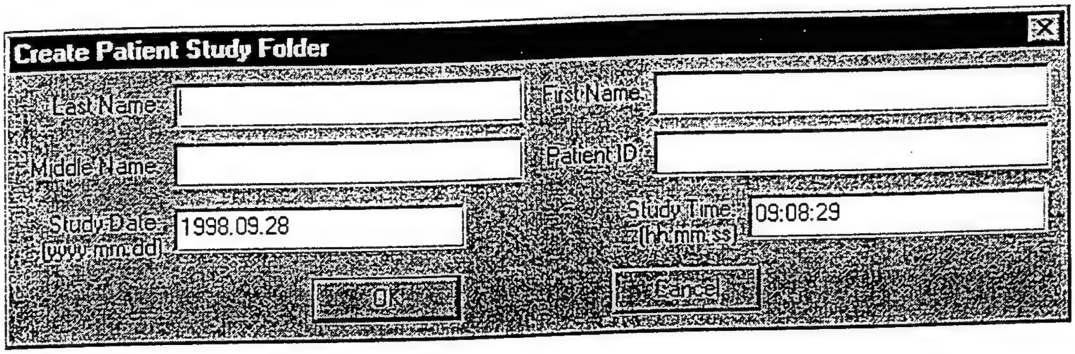
When creating a New Study, a patient's folder consisting of patient information and images will be created. This folder may be viewed and/or sent to a remote machine.

1. Run **VIEWSEND Medical** (double click VIEWSEND Medical icon)

2. On the main Toolbar click on the **New Study** button.



3. Enter patient's name and identification (if known).



Last Name:

First Name:

Middle Name:

Patient ID:

Study Date (yyyy.mm.dd): 1998.09.28

Study Time (hh:mm:ss): 09:08:29

* If ID is not entered, the program will automatically generate one.

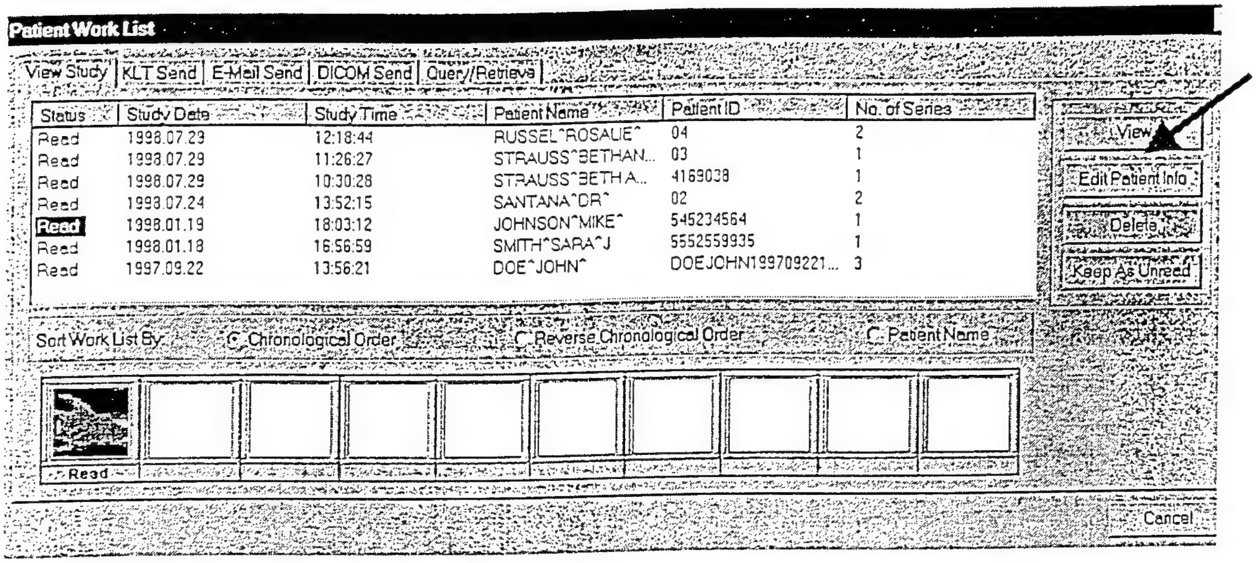
How to Take a Snapshot and Add to a Study

For capturing a still image from the video screen.

1. **Open** a Study (See **How to Open A Study**).

2. Select a **Patient**.

3. Click **View**.



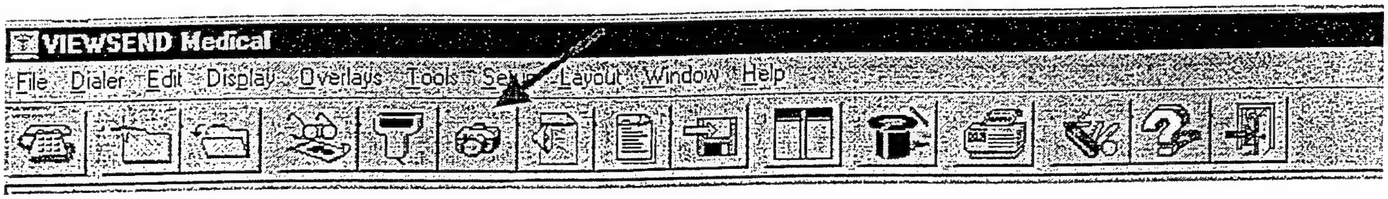
Patient Work List

View Study | KLT Send | E-Mail Send | DICOM Send | Query/Retrieve

Status	Study Date	Study Time	Patient Name	Patient ID	No. of Series
Read	1998.07.23	12:18:44	RUSSEL^ROSALIE^	04	2
Read	1998.07.29	11:26:27	STRAUSS^BETHAN...	03	1
Read	1998.07.29	10:30:28	STRAUSS^BETH A...	4169038	1
Read	1998.07.24	13:52:15	SANTANA^DR^	02	2
Read	1998.01.19	18:03:12	JOHNSON^MIKE^	545234564	1
Read	1998.01.18	16:56:59	SMITH^SARA^J	5552559935	1
Read	1997.09.22	13:56:21	DOE^JOHN^	DOEJOHN199709221...	3

Sort Work List By: ○ Chronological Order ○ Reverse Chronological Order ○ Patient Name

4. Click **Video Capture** from the toolbar.



VIEWSEND Medical
File Dialer Edit Display Overlays Tools Setup Layout Window Help

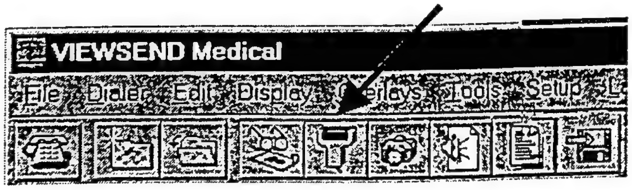
* The snapshot image will be automatically added to the currently opened Patient Study.

How to Digitize a Film and Create or Add to a Study

Note: The scanner has to be turned on BEFORE turning on the computer.

1. Click on **File.**
2. Click on **Select Source.**
3. Select Vidar VXR and click **Select.**
4. Open a Study (See **How to Open A Study).**

Click **Scan** icon from the toolbar.



6. Click **Preview.**

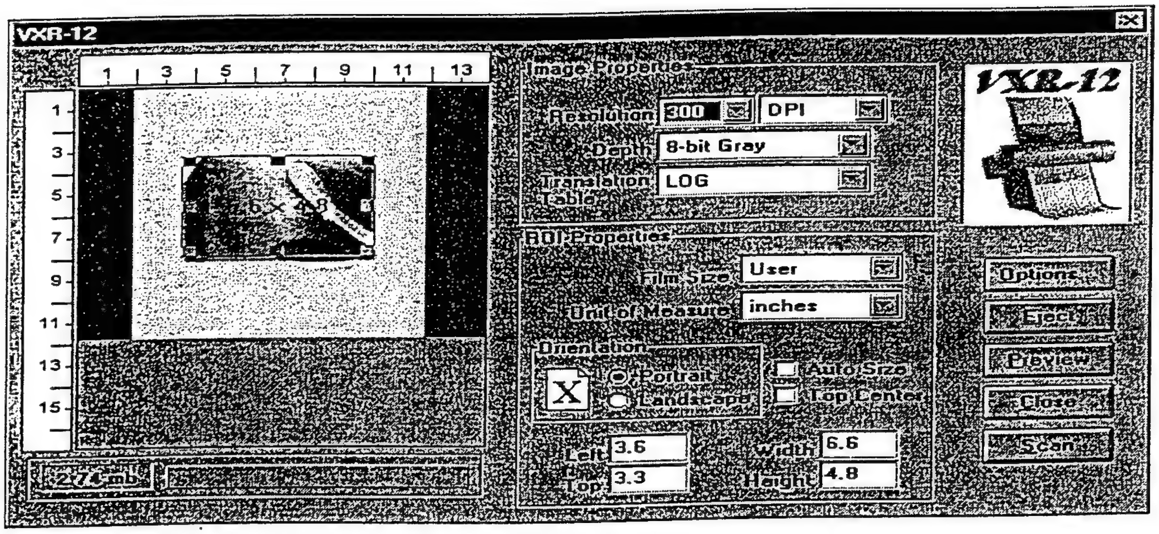

VXR-12

Image Properties

Resolution 300 DPI

Depth 8-bit Gray

Translation Table LOG

ROI Properties

Film Size User

Unit of Measure inches

Orientation

● Portrait

○ Landscape

□ Auto Size

□ Top Center

Left 3.6

Top 3.3

Width 6.6

Height 4.8

7. Adjust Image Frame and click Scan. Image will be automatically added to study.

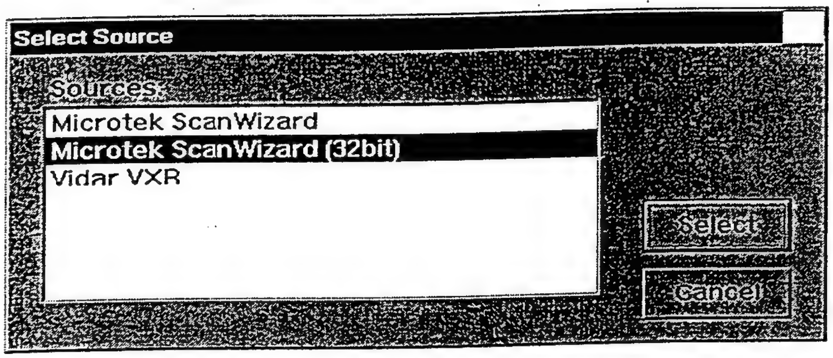
How to Scan a Document and Add to a Study

Note: The scanner has to be turned on BEFORE turning on the computer.

1. Click on **File** from top menu.

2. Click on **Select Source.**

3. **Select** Microtek ScanWizard (32 bit) **from list of sources and click on** Select.

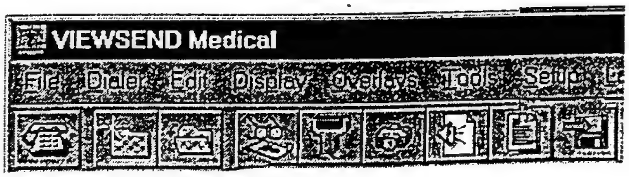


Sources:

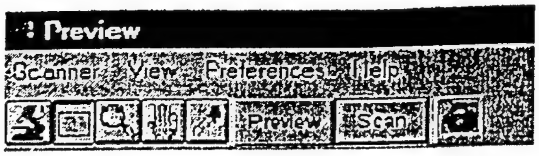
- Microtek ScanWizard
- Microtek ScanWizard (32bit)
- Vidar VXR

4. Open a Study (follow all the steps in **How to Open a Study**).

5. Click on **Scan** Icon.



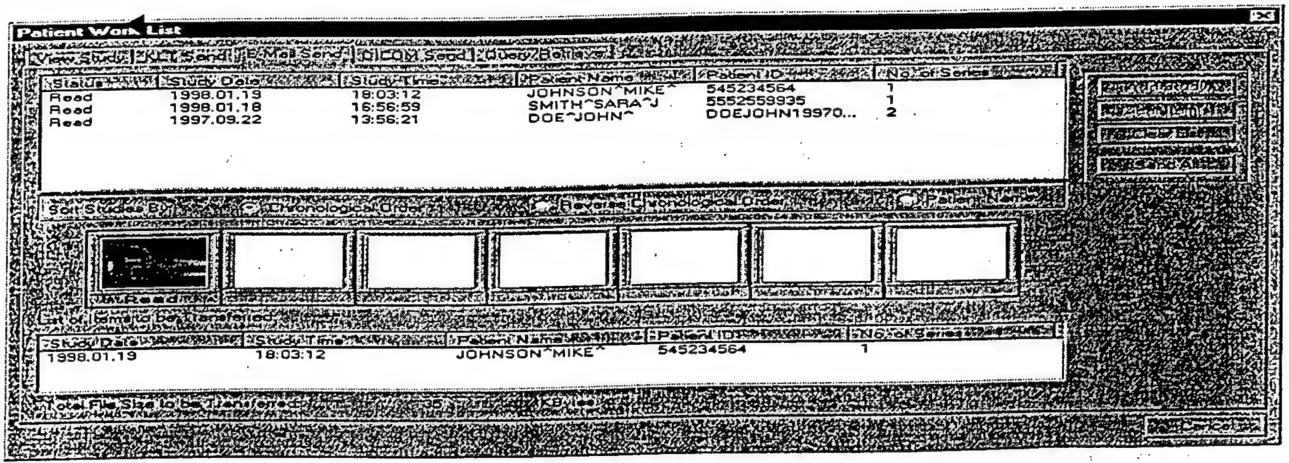
6. Click on **Preview** on the toolbar (one click).



7. Adjust Image Frame and click **Scan.** The document will be automatically added to the selected patient study.

How to Send a Study through IP

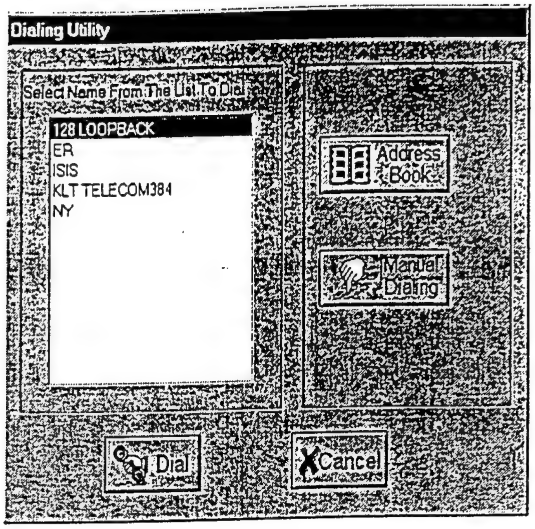
1. Click on the "Open a study" icon (See **How to Open a Study**).
2. Select **KLT Send** tab.
3. Highlight the study you want to send
4. Click on **Add Study**
5. Click on **Send All.**



Status	Study Date	Study Time	Patient Name	Patient ID	No. of Series
Read	1998.01.19	18:03:12	JOHNSON^MIKE^	545234564	1
Read	1998.01.18	16:56:59	SMITH^SARA^J	5552559935	1
Read	1997.09.22	13:56:21	DOE^JOHN^	DOEJOHN19970...	2

Study Date	Study Time	Patient Name	Patient ID	No. of Series
1998.01.19	18:03:12	JOHNSON^MIKE^	545234564	1

6. Select (one click) the party you want to call and press **Dial**.

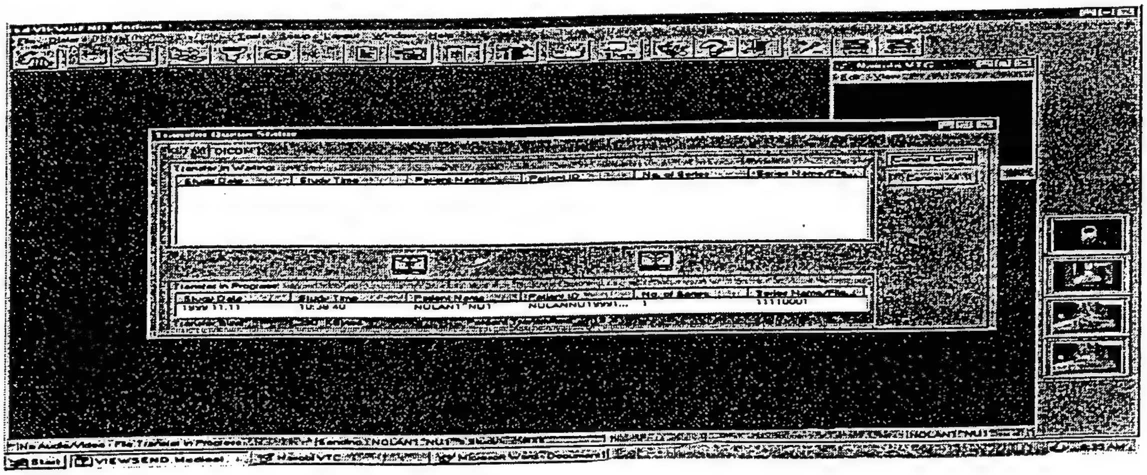


128 LOOPBACK
ER
ISIS
KLT TELECOM384
NY

7. If the party is not in the list of your address book, click **Manual Dialing** and enter the party's name With ISDN or IP adress and click **Dial.**

8. Highlight name and click the **Dial** icon.

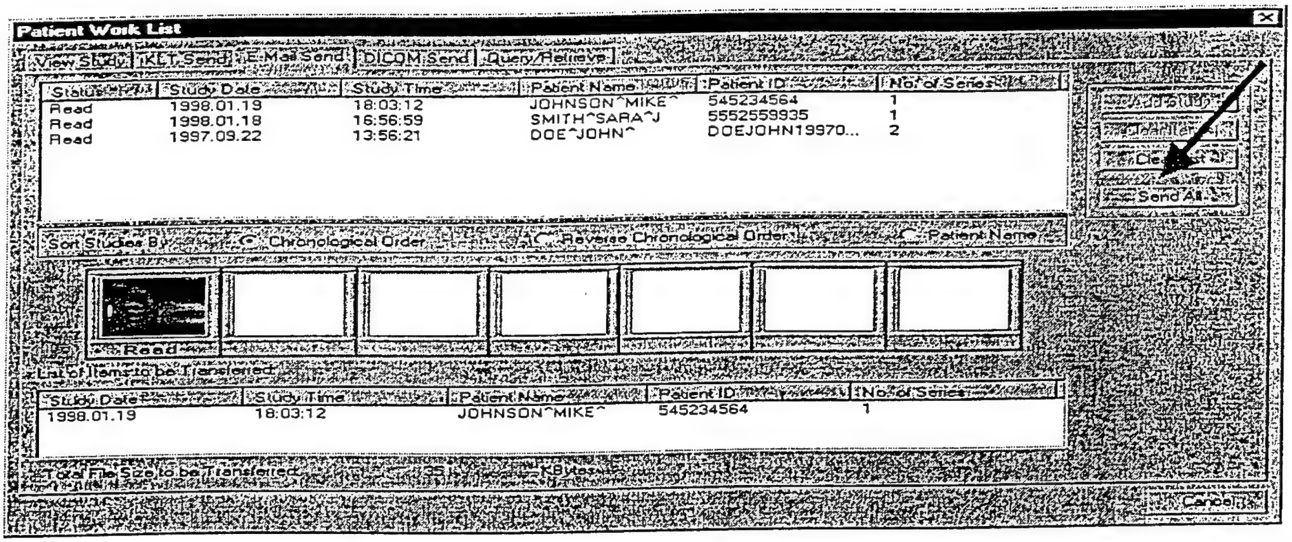
9. The window below shows the normal data transmission during a KLT (or IP) Send



Study Date	Study Time	Patient Name	Patient ID	No. of Series	Series Name/File
1999.11.11	10:38:40	NOLANT NU1	NOLANNU1999...	1	11110001

How to Send a Study through E-Mail

1. Viewsend has the capability to send by e-mail a patient's folder with all the images and patient's information.
2. Open a study (See **How to Open a Study**).
3. Select **E-mail Send** tab.
4. Highlight name.
5. Click on **Add Study**.
6. Click on **Send All**.



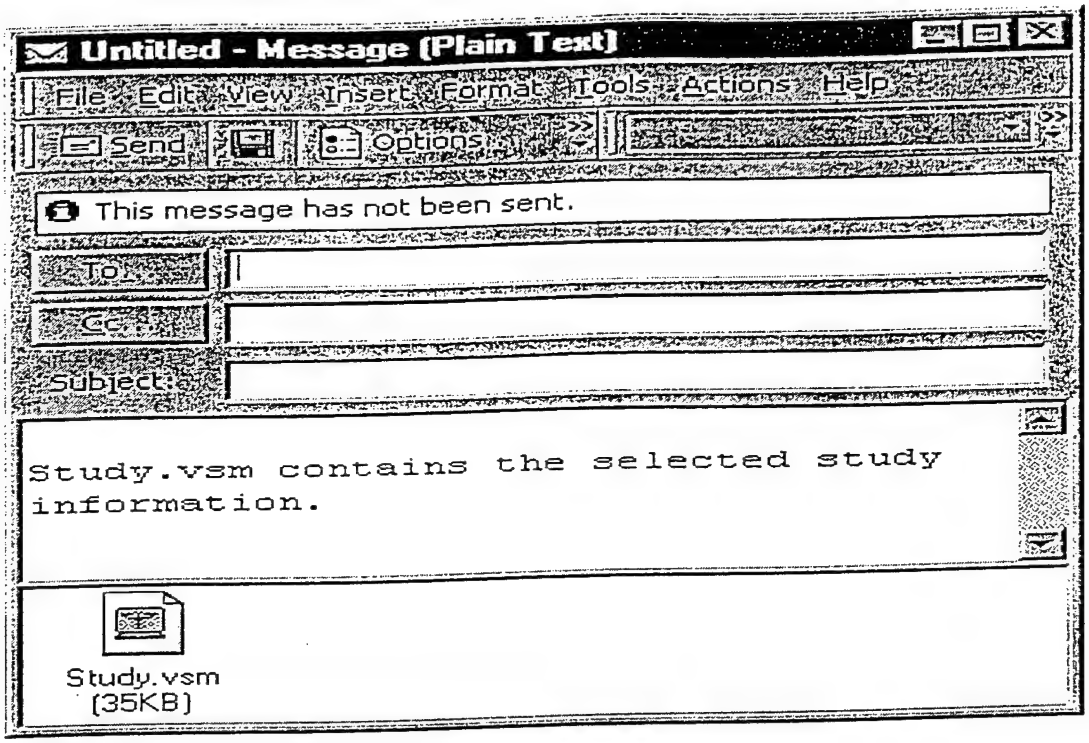
Status	Study Date	Study Time	Patient Name	Patient ID	No of Series
Read	1998.01.19	18:03:12	JOHNSON^MIKE^	545234564	1
Read	1998.01.18	16:56:59	SMITH^SARA^J	5552559935	1
Read	1997.09.22	13:56:21	DOE^JOHN^	DOEJOHN19970...	2

List of Items to be Transferred

Study Date	Study Time	Patient Name	Patient ID	No of Series
1998.01.19	18:03:12	JOHNSON^MIKE^	545234564	1

Total File Size to be Transferred 35 KBytes

7. Choose E-mail program from list and click **OK**.
8. Enter e-mail address of the party to receive the study.
9. Enter the Patient's name in the Subject and press **Send**.
10. To open a study you received by email, open message and double click on **attachment icon**.
11. The default outlook E-mail application will automatically pop up within Viewsend to send the selected study to the remote site.


Untitled - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Send
Options
To...
Cc...
Subject:

This message has not been sent.

Study.vsm contains the selected study information.

Study.vsm (35KB)

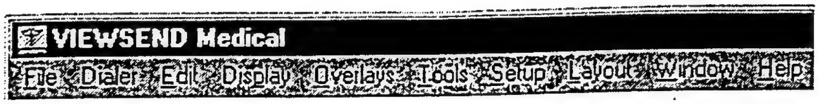
12. The email addresses are as follows for the consultation sites:

Location	Email Addresses
Nairobi Health Unit	KLTNRB@state.gov
MED Washington	VTC@state.gov
ISIS Center	Nairobi@isis.imac.georgetown.edu

Location	Computer Name
MED Washington's KLT Machine	DOS-KLT-MED-01
KLT machine in Regional Medical Office, Nairobi	NRB-KLT-RMO-01
KLT machine in Health Unit, Dar es Salaam (tentative)	DAR-KLT-HU-01

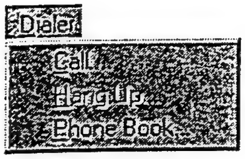
Teleconsulting Tools Available

The main menu tool bar is shown below and a description of the functions available are presented.



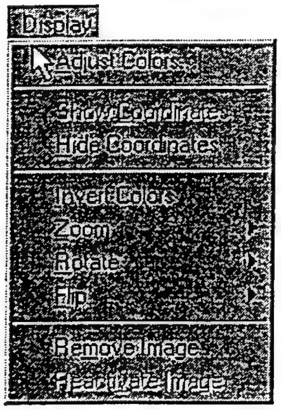
Click any Menu Topic for more information

Main Menu - Dialer



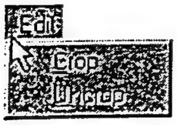
Click any Menu Selection for more information

Main Menu - Display



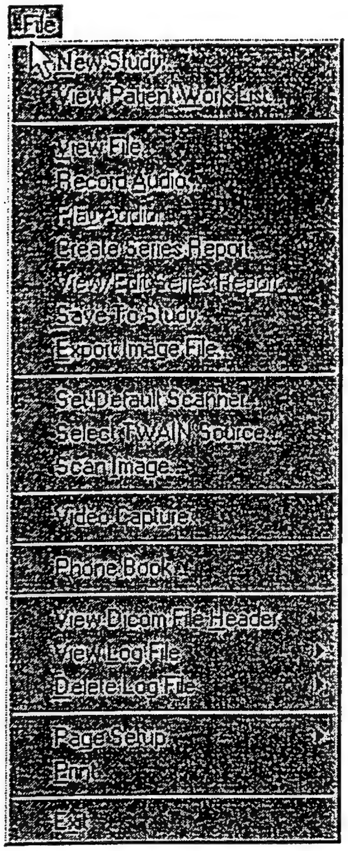
Click any Menu Selection for more information

Main Menu - Edit



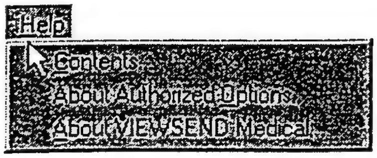
Click any Menu Selection for more information

Main Menu - File



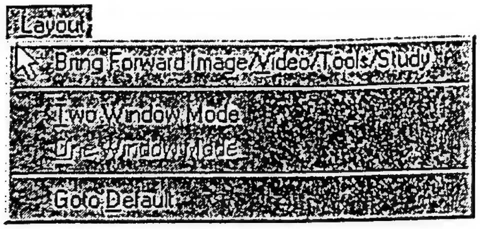
Click any Menu Selection for more information

Main Menu - Help



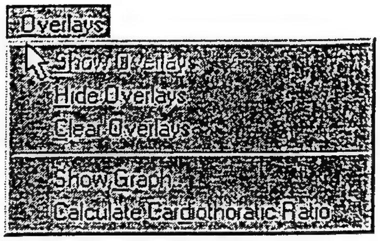
Click any Menu Selection for more information

Main Menu - Layout



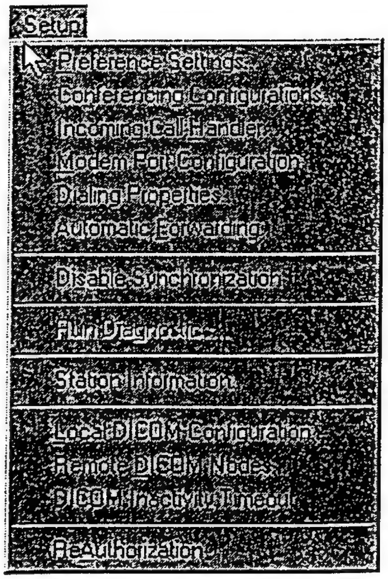
Click any Menu Selection for more information

Main Menu - Overlays



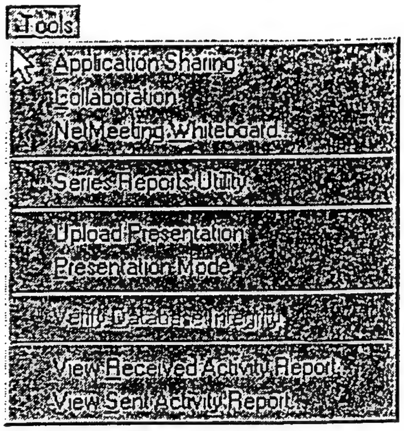
Click any Menu Selection for more information

Main Menu - Setup



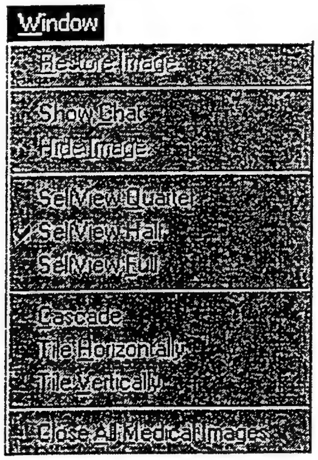
Click any Menu Selection for more information

Main Menu - Tools



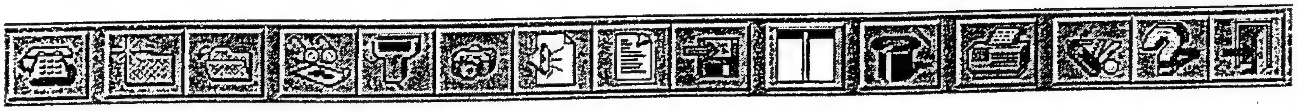
Click any Menu Selection for more information

Main Menu - Window



Click any Menu Selection for more information

Toolbar Commands



Click any Toolbar Command Icon for more information

Toolbar Command - Bring Forward Image/Video/Tools/Study

Brings hidden windows back into view (For example, the tool palette, thumbnail image and video windows may have been hidden by various actions).

Toolbar Command - Conference Config

Provides three tabs for setting Audio devices, Camera Control Interface and System Options including auto-answering non-modem type calls.

Toolbar Command - Create Series Report

Creates or opens a document saved with the study that contains a wealth of information about the study, including series images. Primarily intended for producing a printed output report, the series report serves a dual purpose of allowing various notes to be added to the study.

Toolbar Command - Display Help File

Displays the VIEWSEND Medical help file in the new Windows tri-pane format (Books and Topics displayed in a left window and content in a right window).

Toolbar Command - Exit VIEWSEND Medical

Gracefully closes the VIEWSEND Medical application.

Toolbar Command - New Study

Opens the "Create Patient Study Folder " window. This command button will be used only under special circumstances, such as creating a folder to hold images for a training class.

Toolbar Command - Phone

Used to place a Call, Hang-up when complete, or access the phone book for administrative purposes.

Toolbar Command - Print

Initiates the standard Windows print process. If the DICOM print option has been purchased, additional capabilities are available for printing to film.

Toolbar Command - Record Audio

Allows capturing sound, using simple "Record" "Stop" and "Play" controls if the PC is equipped with a sound system (including a microphone or other input device).

Toolbar Command - Save To Study

Saves the current active series image(s) or external graphic file being viewed to the study. Allows annotated copies of the same image to be saved as additional images in the study.

Toolbar Command - Scan Image

Starts in motion the process of acquiring an image from a TWAIN device (like a VIDAR scanner). The scanner must be turned on BEFORE the PC is turned on.

Toolbar Command - Two Window Mode

Switches between a single window and two windows when the "*Maximum Number of Image Windows Opened Allowed*" option is set for "*Two Windows Only*" in *Setup – Preference Settings – Display*

In the multi-window mode, this button will arrange open windows based on *Main Menu - Preference Setting Display Tab Default Window Arrangement.* For example, "Tile Vertical ".

Toolbar Command - Video Capture

Ordinarily not used with VIEWSEND Medical, but allows taking a 'snapshot' of any video image available if the PC is equipped with a video capture card.

Toolbar Command - View File

Opens a 'Windows Explorer' like window to preview and select a graphic image file (.bmp, .jpg, .gif) for inclusion in the active study.

Toolbar Command - View Patient Work List

Opens the "Patient Work List " window from which a study may be selected. Also the on-call physician will use this button, after arriving at the medical facility, to review any studies sent to him/her via RIX.

Using VIEWSEND Medical

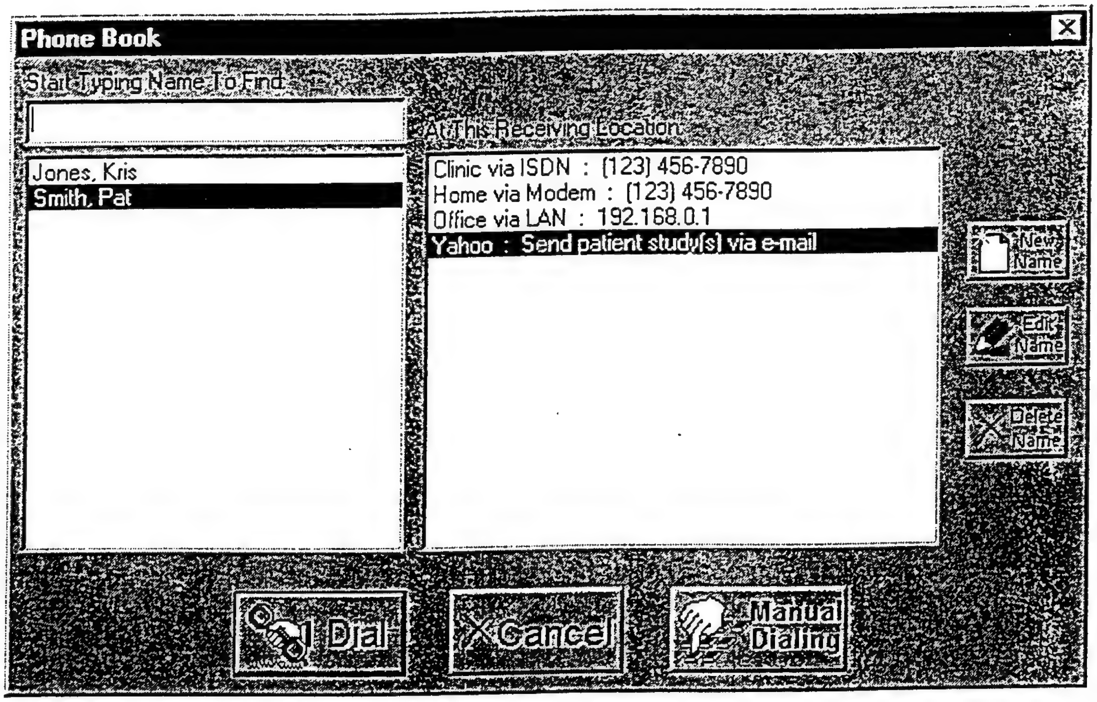
Answering Calls

There are two places in VIEWSEND Medical that deal with auto-answering incoming calls based on the type of communication facility used (Modems or LAN/WAN). It is possible to have VIEWSEND Medical set to auto-answer BOTH modem and LAN/WAN calls (of course only ONE call will be active at any instant in time). In other words, both types of calls can be READY to auto-answer, but once a call is accepted, the other facility will be ignored until the first call is completed.

For example, if VIEWSEND Medical is used for video conferencing and for receiving RIX calls, the auto answer setting in "*Main menu – Setup – Conferencing Configurations – System Options Tab*" controls the LAN/WAN video call auto-answer feature. At the same time, the setting in "Main Menu - Setup - Incoming Call Handler " controls auto-answer for RIX through the modem.

Making a Call

To make a call, click on the Phone Toolbar Command Button ☎ or select "Main Menu – Dialer – Call". Highlight (single-click) the name of the person you wish to call and the location (if multiple locations are available for the same person). Click the "Dial" button to place the call. For details on adding a name or location, refer to "Using the Phone Book ".



Phone Book

Start Typing Name To Find

Jones, Kris
Smith, Pat

At This Receiving Location:

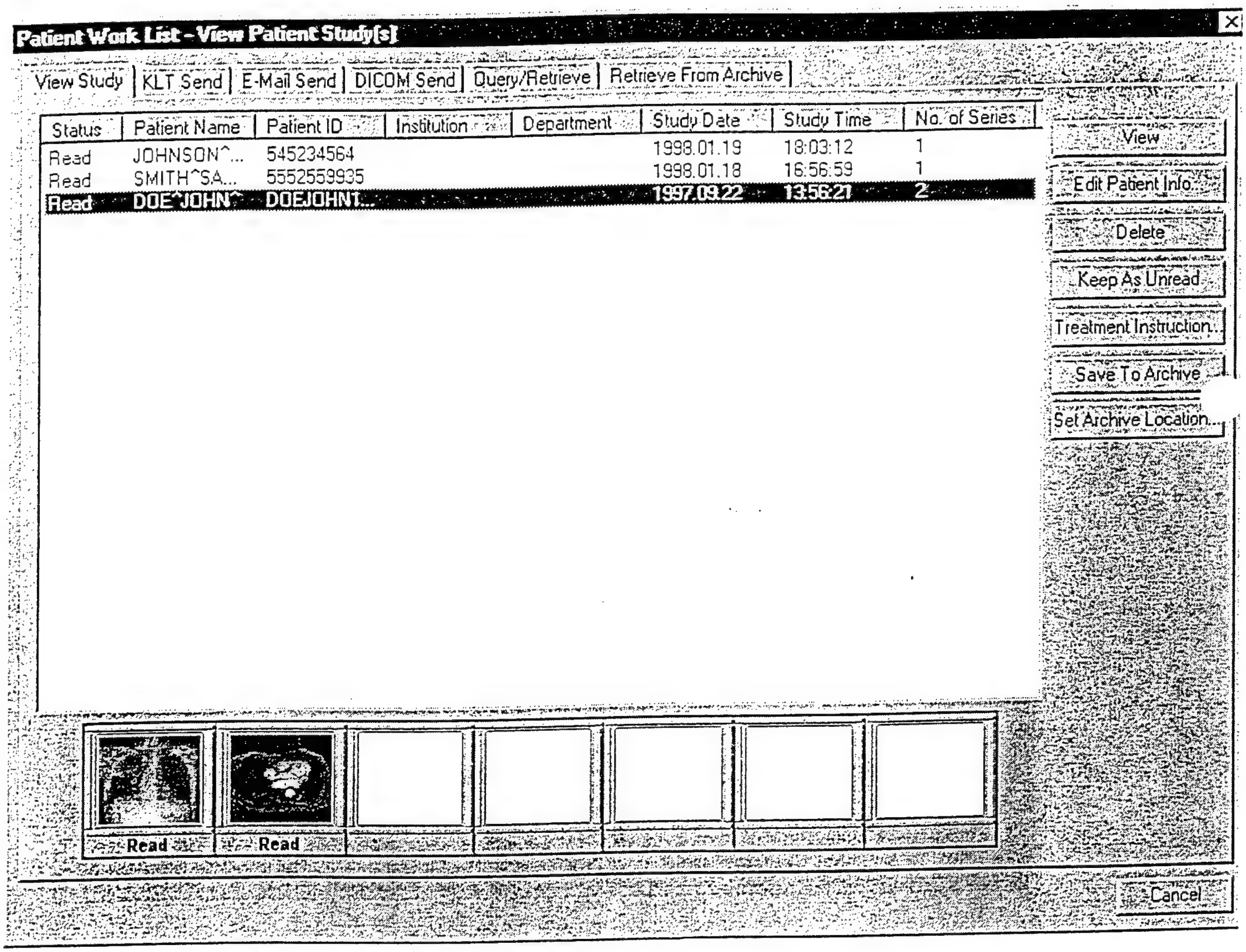
Clinic via ISDN : (123) 456-7890
Home via Modem : (123) 456-7890
Office via LAN : 192.168.0.1
Yahoo : Send patient study(s) via e-mail

To end the call, click on the Phone Toolbar Command Button ☎ or select "Main Menu – Dialer – Hang Up"

Viewing Images

Images are captured at the sending end and saved in a series. Some medical devices bundle multiple images into a single series, while other devices capture only a single image in a series. It is the series that gets sent to the VIEWSEND Medical receive station and is stored in a patient study. A Patient Work List is used to select any given study with which to work.

To open the Patient Work List, click on the icon located on the main toolbar (third icon from the left). You will see:



Patient Work List - View Patient Study[s]

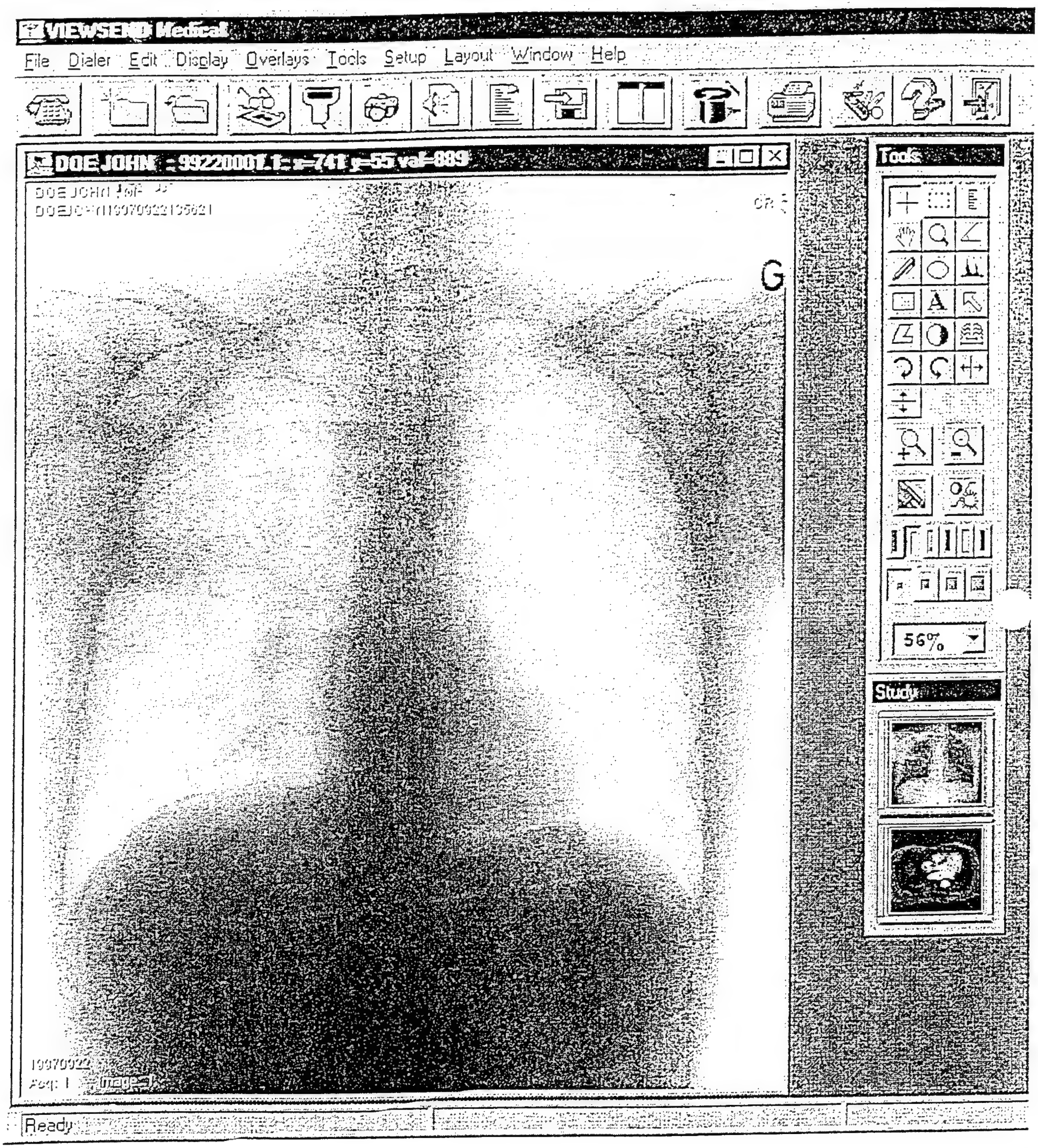
Status	Patient Name	Patient ID	Institution	Department	Study Date	Study Time	No. of Series
Read	JOHNSON^...	545234564			1998.01.19	18:03:12	1
Read	SMITH^SA...	5552559935			1998.01.18	16:56:59	1
Read	DOE^JOHN^	DOEJOHN1...			1997.09.22	13:56:21	2

Single-click on the desired study in the list to see thumbnail views of all series contained in the study.

Begin working with the study in one of several ways. Single click the study entry (thumbnail views of the series will appear) then click the "View" button while the series is highlighted. Or, simply double-click on the study entry in the Patient Work List. Using this method, the *first* series will be immediately available (full Size) and thumbnail views of all images will be displayed along the lower right side of the working window.

To start working with a *specific* series, rather than the first one listed, single-click a study to show thumbnail views. Then double-click on the thumbnail of the *exact* series desired or single click the *exact* series thumbnail (it will then be framed in a contrasting color) then click the "View" button.

The Working Window

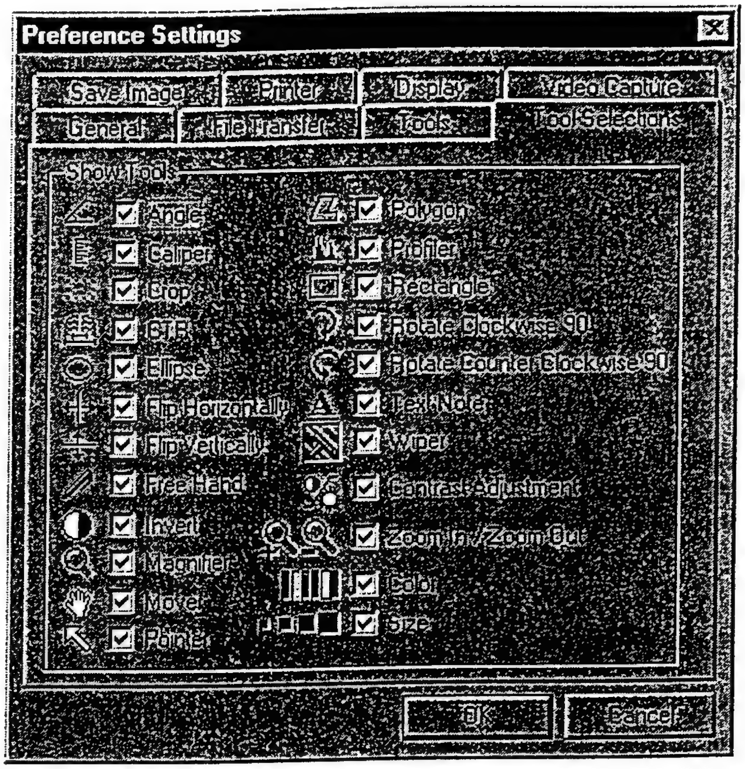


Double-click any thumbnail image to work with it. (You may need to scroll to see all of the thumbnail images along the lower right side of the window).

Tip: More than one series can be open at one time. When used in conjunction with the ◫ icon, a 'before and after' comparison can be made.

Setting Tool Preferences

After you have tried all of the tools on the Tool Palette, you may wish to remove those you seldom use. It is very easy to add and remove tools on the palette at any time using "*Main Menu – Setup – Preference Settings – Tool Selections Tab*"



☑ Angle
☑ Caliper
☑ Crop
☑ CTR
☑ Ellipse
☑ Flip Horizontally
☑ Flip Vertically
☑ Free Hand
☑ Invert
☑ Magnifier
☑ Move
☑ Pointer
☑ Polygon
☑ Profiler
☑ Rectangle
☑ Rotate Clockwise 90
☑ Rotate CounterClockwise 90
☑ Text Note
☑ Wiper
☑ Contrast Adjustment
☑ Zoom In/Zoom Out
☑ Color
☑ Size

Acquiring Information

Scanner & Other TWAIN Devices

Acquire an Image from Scanner

Insure that a TWAIN compatible interface scanner is properly installed and *Main Menu – File - Set Default Scanner* has "TWAIN compatible" selected or select Lumisys if appropriate.

1. Select a scanner source.

From *Main Menu – File - Select Source* select the Vidar VXR-12 or other installed scanner

2. Either click *Main Menu – File – Scan Image* or click the Toolbar Command button

   Note

   When you are in a conference, a newly acquired scanned image will be transferred to the remote workstation and will be automatically loaded into the working window.

Scopes, Cameras & Other Video Devices

Video devices (such as the AMD ExamCam or the American Dental Technologies UltraCam Intraoral Camera) may be used as an input to VIEWSEND Medical. Using the optional WINNOV capture card. images may be captured and stored as series in a study.

When utilizing the WINNOV card, either NTSC or S-Video inputs may be used. Use the Video Capture preference setting to select WINNOV as the capture source.

Audio

An audio recording may be added to a study if the PC is equipped with recording and playback capabilities.

With a patient folder and study open, click the icon to activate the recorder interface.

Record, Stop, and Play buttons will be available. Please note that the recording may not be appended. Clicking the RECORD button a second time will replace the existing recording. Audio recordings become part of the study and are transported with the study automatically.

Query/Retrieve From a DICOM Server

Works with DICOM 3.0 compliant servers. Query requires a connection to a DICOM server. Retrieve/Read may use a server or be a peer to peer function.

Before using the Query function, you should consult with your DICOM server administrator to make certain your settings are correct.

Image Files Outside VIEWSEND Medical

Main Menu - File - View File

With a patient folder open, click This will activate an explorer-like interface that will allow selection of a graphical image. Imported images are restricted to types .jpg, .gif and .bmp. Images must be saved to the patient study or they will be discarded.

Saving Acquired/Modified Images To a Study

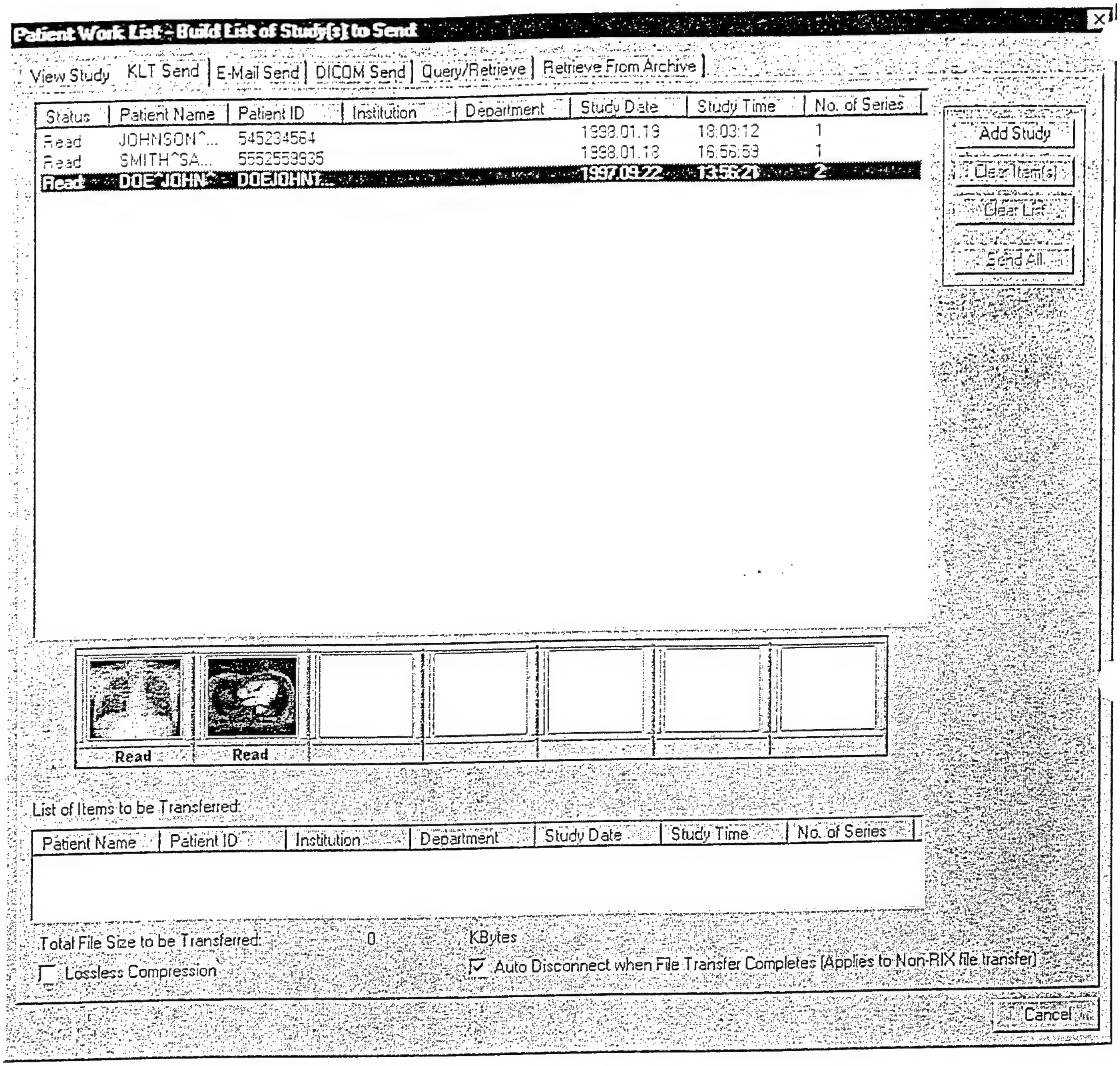
To save as a new series after viewing or modifying an image, click the Toolbar Command Button.

The saved image is dependant on compression type and quality factor set using the Main Menu - Setup - Preference Settings- Save Image. These settings remain in effect until changed.

Sending Information

KLT Send

Used to send selected patient information to a remote site using a proprietary transmission protocol



Status	Patient Name	Patient ID	Institution	Department	Study Date	Study Time	No. of Series
Read	JOHNSON^...	545234564			1998.01.13	18:03:12	1
Read	SMITH^SA...	5552553935			1998.01.13	16:56:59	1
Read	DOE^JOHN^...	DOEJOHNT...			1997.09.22	13:56:21	2

List of Items to be Transferred:

Patient Name	Patient ID	Institution	Department	Study Date	Study Time	No. of Series

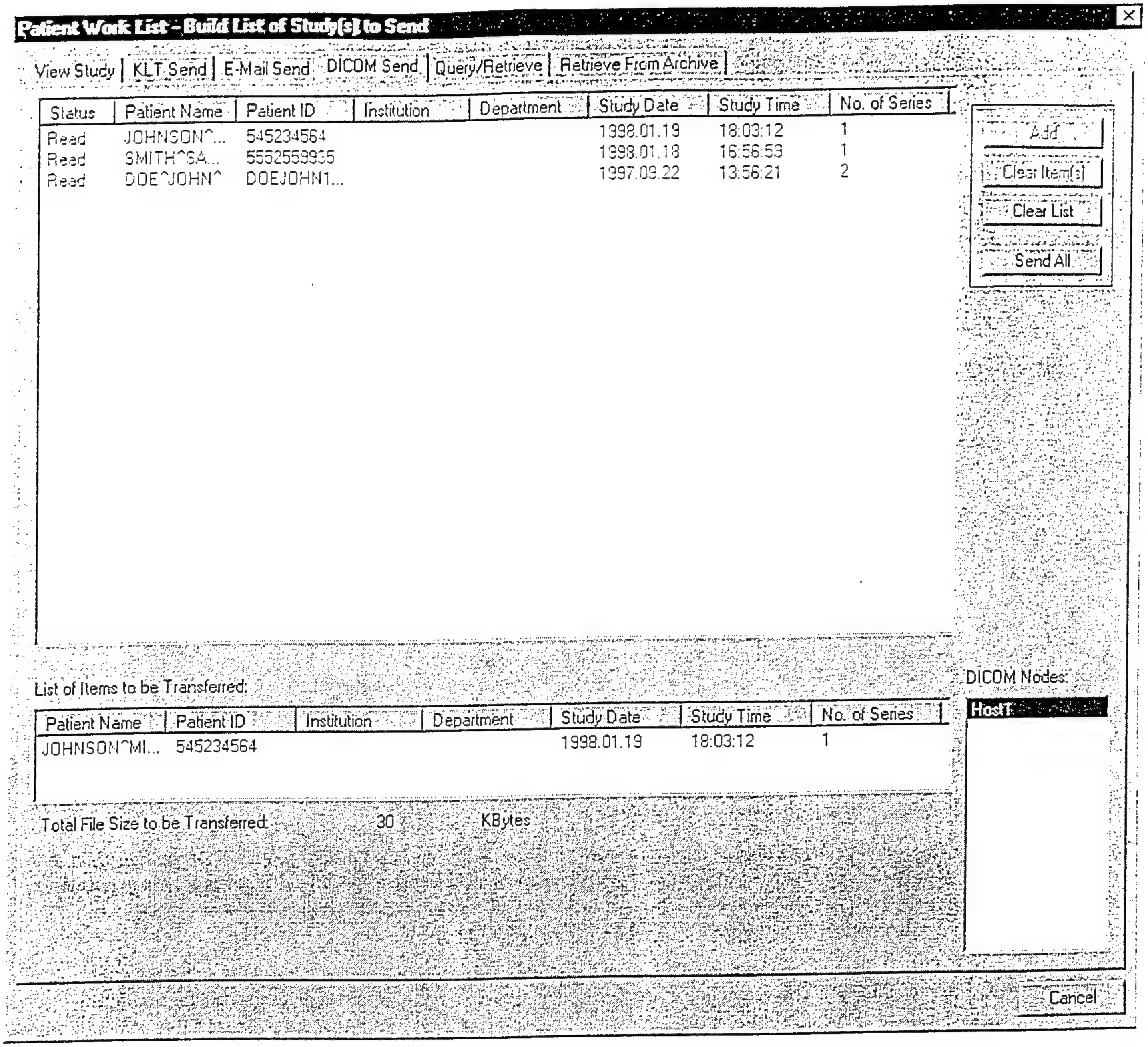
Total File Size to be Transferred: 0 KBytes

☐ Lossless Compression

☑ Auto Disconnect when File Transfer Completes (Applies to Non-RIX file transfer)

DICOM Send

Used to send selected patient data to a remote site or to a modality using the DICOM 3.0 standard. DICOM Send may also be used for peer to peer operation without the use of a DICOM Server. DICOM must be properly configured before using this send option



Status	Patient Name	Patient ID	Institution	Department	Study Date	Study Time	No. of Series
Read	JOHNSON^...	545234564			1998.01.19	18:03:12	1
Read	SMITH^SA...	5552559935			1998.01.18	16:56:59	1
Read	DOE^JOHN^	DOEJOHN1...			1997.09.22	13:56:21	2

List of Items to be Transferred:

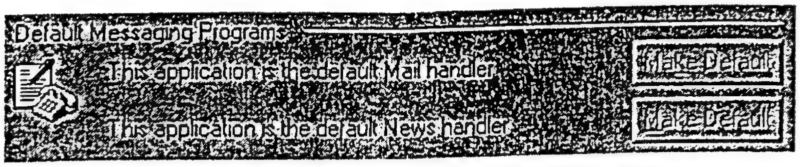
Patient Name	Patient ID	Institution	Department	Study Date	Study Time	No. of Series
JOHNSON^MI...	545234564			1998.01.19	18:03:12	1

Total File Size to be Transferred: 30 KBytes

E-Mail

Study information can be sent as an attachment to an E-mail message. The PC default mail package is always used, therefore it is important to insure that it works properly before sending e-mail from VIEWSEND Medical.

Even if your mail program works well as a stand-alone program and you can send E-mail from the PC with no problems, you must further insure that your E-mail program has been set as the "Default" mail handler for Windows. For example, in Outlook Express 5.0 the option is set from the *Main Menu - Tools - Options - General Tab.*



Default Messaging Programs

This application is the default Mail handler

This application is the default News handler

As a quick check to see if programs on the PC have direct access to the mail package, run the WordPad program that came with Windows Accessories. Select *Main Menu - File - Send.* If a new e-mail message is created, the e-mail will probably work with VIEWSEND Medical.

E-mail has not been tested extensively with all off-the-shelf mail packages but should work with most programs.

How To Send E-Mail

E-mail can be sent in one of two ways: 1) Through the phone book, or 2) Through the E-mail Send Tab on the Patient Work List.

1. VIEWSEND Medical ***Phone Book*** Method - Where the destination location use the E-mail *Calling Method,* the study(s) is sent as an attachment. The default mail program will be launched automatically by VIEWSEND Medical, the file(s) is already attached, and a standard message is included in the message body. The sender need only fill in the To: and Cc: information and optionally add text to the message body if desired. The phone book is invoked when sending a study(s) from the KLT Send Tab.

2. ***E-mail Tab*** Method – From the E-Mail Tab, studies to be sent are selected and the default E-Mail program is launched without going through the VIEWSEND Phone Book.

Auto-Forwarding

Main Menu – Setup – Automatic Forwarding

Use this option to enable/disable auto-forwarding images using either the DICOM send or KLT Send method. A list of available destinations is presented from which one may be chosen (E-Mail destinations are not available because they require manual interaction with the PC default E-mail program). When enabled, all images received on the station will be sent directly to the designated recipient.

Only DICOM images can be forwarded when a modem is being used to contact the recipient (Calling Methods ZModem and FTP). This restriction exists because images from non-DICOM sources may make the modem unavailable for outbound calling.

Dialer

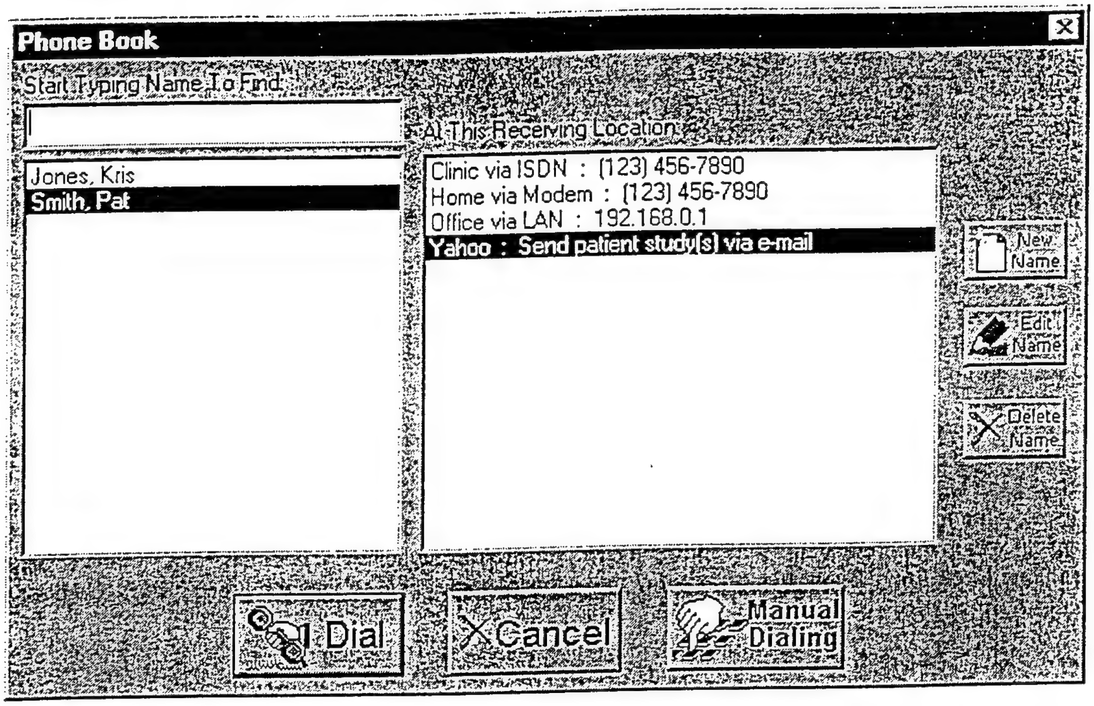
Main Menu – Dialer items are used to initiate a *Call* and to *Hang-up* when the call is completed. New names and locations may also be added to the *Phone Book*. Clicking the Phone Toolbar Command Button ☎ is the easiest way to access dialer functions.

Phone Book

Using the Phone Book

All calls are made from the phone book window. The phone book is accessed either from *Main Menu - Dialer – Phone Book* or by clicking the phone *Toolbar Command* button ☎.

In normal use, the phone book will be opened automatically by clicking the *Toolbar Command* button to place a call. However, opening the phone book when not placing a call is useful for 1) adding a name before it is needed (i.e. adding all on-call names at one time), 2) adding more locations to an existing physician's entry, or 3) updating location, pager or other information.



Phone Book

Start Typing Name To Find:

Jones, Kris
Smith, Pat

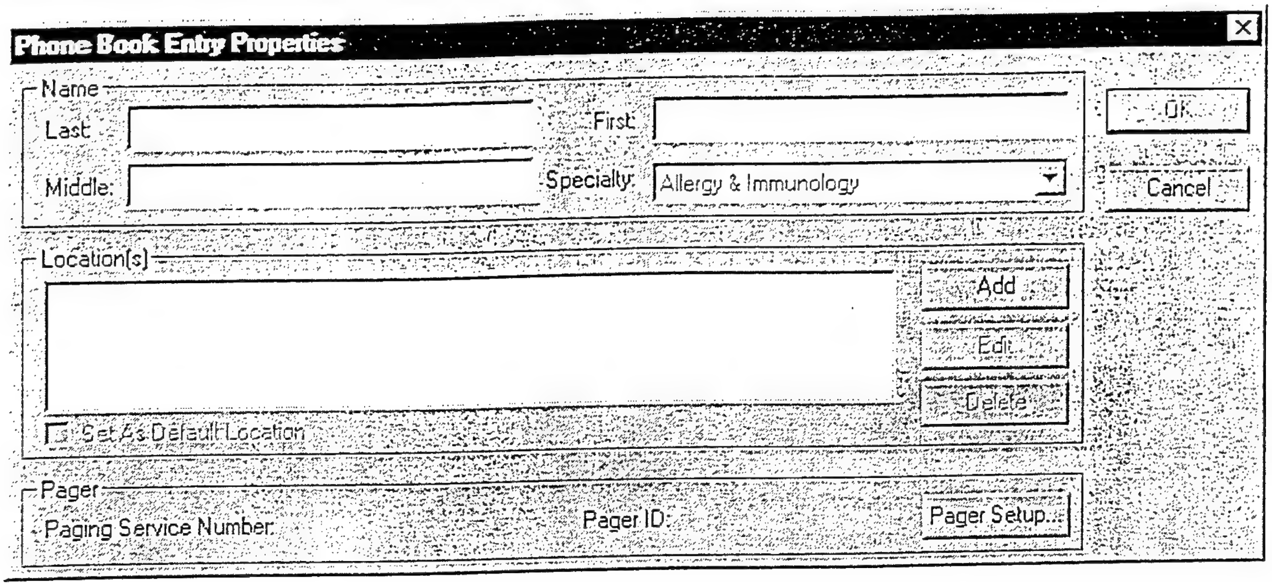
At This Receiving Location:

Clinic via ISDN : (123) 456-7890
Home via Modem : (123) 456-7890
Office via LAN : 192.168.0.1
Yahoo : Send patient study(s) via e-mail

From this initial phone book screen, a call can be placed (this is the most frequent use), new entries may be made and existing entries modified.

The "Dial" and "Manual Dialing" buttons are available (non-gray) and disabled based on the communications methodology associated with each location . For example, the Dial and Manual Dial buttons will be available immediately if the chosen location is on a LAN/WAN via IP. In other words, it is always necessary to start by placing a call, so the buttons are available. If, on the other hand, the chosen location is a RIX station, the Dial and Manual Dial buttons will only be available when a study is in queue waiting to be sent.

Phone Book Entry Information



Specialty: Allergy & Immunology

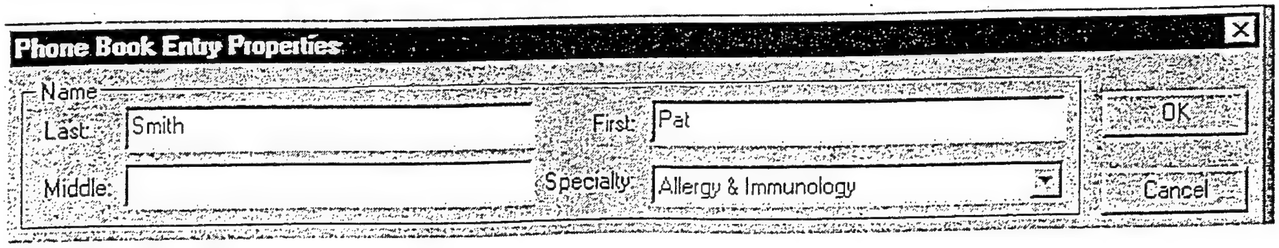
Notice that there are three major sections in this window: 1) Name Section – Consisting of First, Last and Middle name and a pick list for choosing a specialty. 2) Location Section – With its own set of Add, Edit and Delete buttons for adding or making changes to an existing location and a 3) Pager Section – with its own button for working with pager setup information.

Each entry in the phone book will contain a unique name with only one pager setup for that person. However, each person/entry may have multiple locations. This is why the Location section of the Phone Book Entry Properties form has its own set of buttons. The location section of the Phone Book Entry Properties window only displays the final results of work done in the separate "Location Properties" window. Understanding this relationship will avoid confusion when adding a new name to the phone book. The "OK" and "Cancel" buttons on the Phone Book Entry Properties form apply to the single name, single pager and MULTIPLE locations as a group of information

Adding a Name

Access the phone book and click the New Name button New Name. The "Phone Book Entry Properties " screen will appear to allow Name. Location and Pager information manipulation.

Step 1 - In the "Name" section of this form, enter Last Name, First Name, Middle Name/Initial and choose the appropriate specialty.



Last: Smith

First: Pat

Specialty: Allergy & Immunology

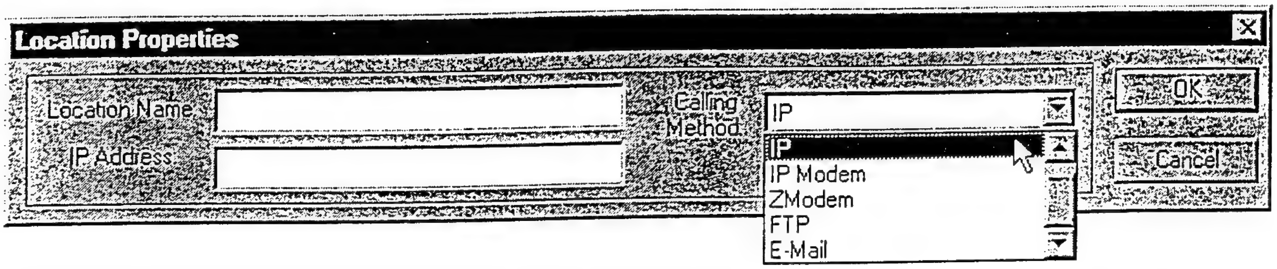
Step2 – In the Location(s) section, click the "Add" button and fill in the appropriate information. See "Adding a Location " for details. Do not be confused by the fact that a separate box appears for location information, you are still in the middle of adding a name to the phone book.

Step 3 – Optionally, complete the Pager Setup for this name.

Step 4 – Click the OK button to the right of the First Name field to finish adding the name to the phone book.

Adding a Location

Access the Phone Book. Clicking the "**Add**" button, or highlighting an existing location and clicking the *Edit* button in the *Location"* Section of the Phone Book Entry Properties form will display the following window:



Location Name and *Calling Method* items will always appear the same in this window, but the third item will vary based on the *Calling Method* selected. For example, Zmodem requires a "*Telephone Number*", FTP requires a "*IP Address*" and E-Mail needs an Internet style *"E-Mail Address"*. The screen label for this third element will change dynamically.

Also note that the selections available in the *Calling Method* box will vary based on the capabilities of the product installed. For example, even though FTP uses an IP address, RJX does not support other IP type functions. Therefore, choices for IP and IP Modem will not appear in the *Calling Method* list for RJX.

Calling Methods :

H320 Used when a dedicated H.320 session is used

Automatic Used for IP based connections. Will accept either an IP address or a name to be resolved by the DNS server on the network.

IP Used on IP based connections (H.323; LAN/WAN) and requires an IP address

IP Modem Rarely used. Allows IP protocol to be used after a call is established over a modem

ZModem Standard modem-to-modem call for file transfer using KLT proprietary protocol

FTP Also a modem-to-modem call but using FTP protocol

E-Mail Launches the PCs default mail package during the send process to attach VIEWSEND files to an E-mail message. Uses the E-mail package address book rather than the VIEWSEND phone book to obtain the recipient's E-mail address.

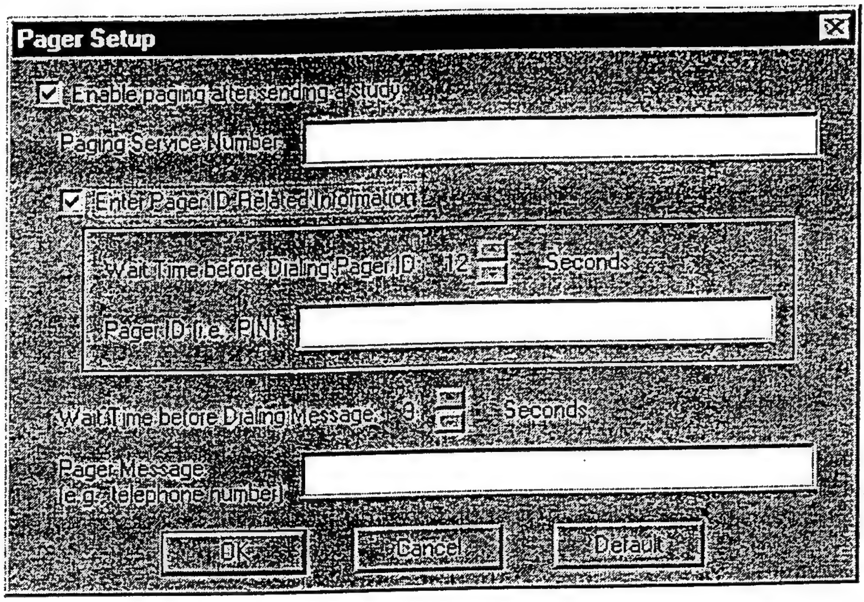
A single name entry in the phone book can have any number of locations. For example, a physician may typically have both a home and office location listed and perhaps a third for e-mail.

Change Name, Location or Pager information

Access the Phone Book and click the "*Edit Name*" button Edit Name to display the Phone Book Entry Properties screen. Follow the procedures for adding a Name, Location or Pager Setup.

Pager Setup

Access the Phone Book and click either the "*New Name*" or "*Edit Name*" button as appropriate. Clicking the "*Pager Setup*" button on the Phone Book Entry Properties screen will allow pager information to be added or changed using the following screen:



☑ Enable paging after sending a study

Paging Service Number:

☑ Enter Pager ID Related Information

Wait Time before Dialing Pager ID: 12 Seconds

Pager ID (i.e. PIN):

Wait Time before Dialing Message: 9 Seconds

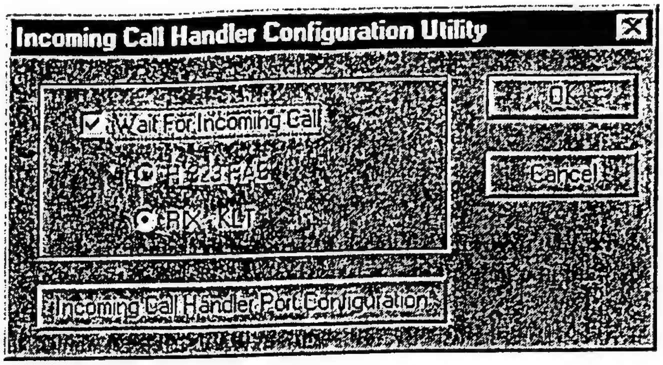
Pager Message: (e.g. telephone number)

Only <u>ONE</u> pager setup is allowed for each name in the phone book. The pager will be activated regardless of which *location* is selected. Unfortunately, due to the wide variation of pager services, configuring the pager is more art than science. Work with your pager service and use trial and error techniques until the pager works satisfactorily.

Receiving Information

Incoming Call Handler

Main Menu - Setup - Incoming Call Handler



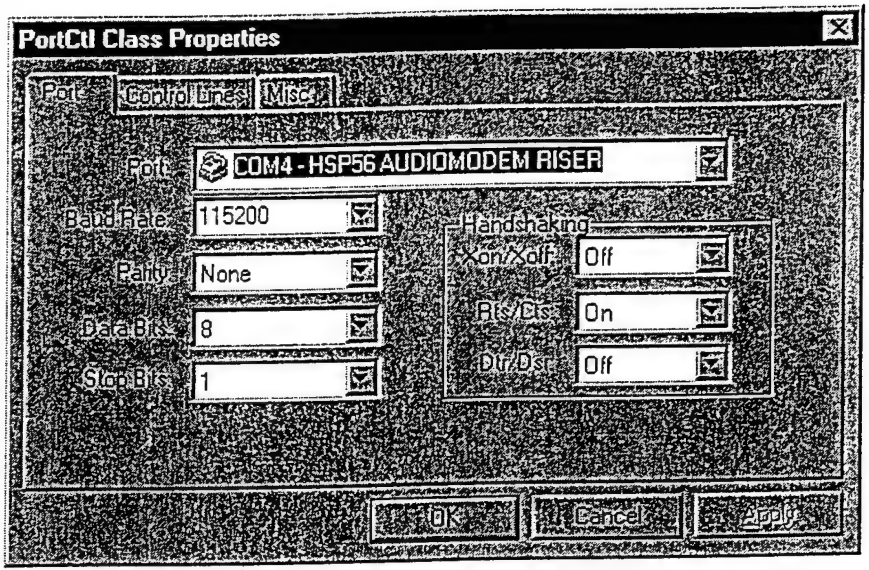
Incoming Call Handler Configuration Utility

☑ Wait For Incoming Call

○ H.323 RAS

● RIX - KLT

This utility is one of two used to set auto-answer capability in VIEWSEND Medical. It controls calls using the PCs modem. When the "Wait For Incoming Call box is checked, auto-answer is enabled for the modem. The H.323 RAS option is rarely used, but allows low quality video and audio to work (marginally) using IP protocol over a standard modem call. Normally, the modem will be used for "RIX – KLT" operations. In this mode, RIX stations calling this VIEWSEND Medical station will be answered and study information transfer using the KLT Send proprietary protocol will occur automatically. Port configuration is also possible from this screen.



PortCtl Class Properties

Port: COM4 - HSP56 AUDIOMODEM RISER

Baud Rate: 115200

Parity: None

Data Bits: 8

Stop Bits: 1

Handshaking

Xon/Xoff: Off

Rts/Cts: On

Dtr/Dsr: Off

For a description of the relationship between this auto-answer utility and the second one used for LAN/WAN auto-answer, see "Answering Calls " in the "*Getting Started*" " – "*Using VIEWSEND Medical*" Help Book

Working With Studies

New Study

A new study can be created in several ways.

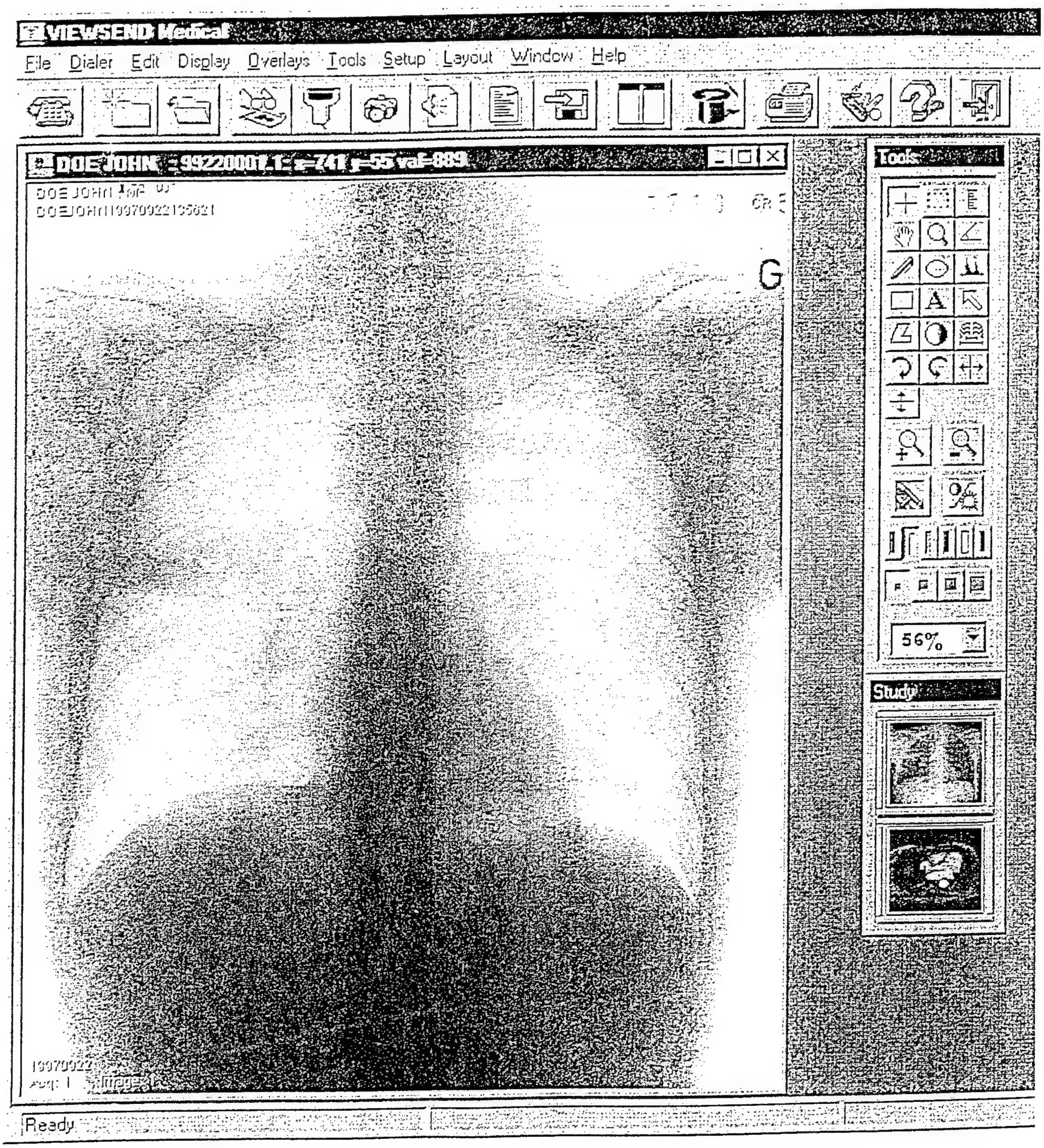
1. A DICOM modality can have VIEWSEND Medical designated to receive its output, which will be automatically stored by VIEWSEND Medical in a new study

2. Any PC running VIEWSEND Medical software can send study information to any other PC that is also running VIEWSEND software. If the study being sent does not already exist on the receiving machine, one will be created.

3. Using the Toolbar Command button, a new study can be created manually and series' added. This is seldom necessary. One instance where manual creation may be beneficial is in a training environment where a sample study is required in advance.

Patient Study Folder

Pictured here is a single Patient Study Folder displaying the image (series) it contains.

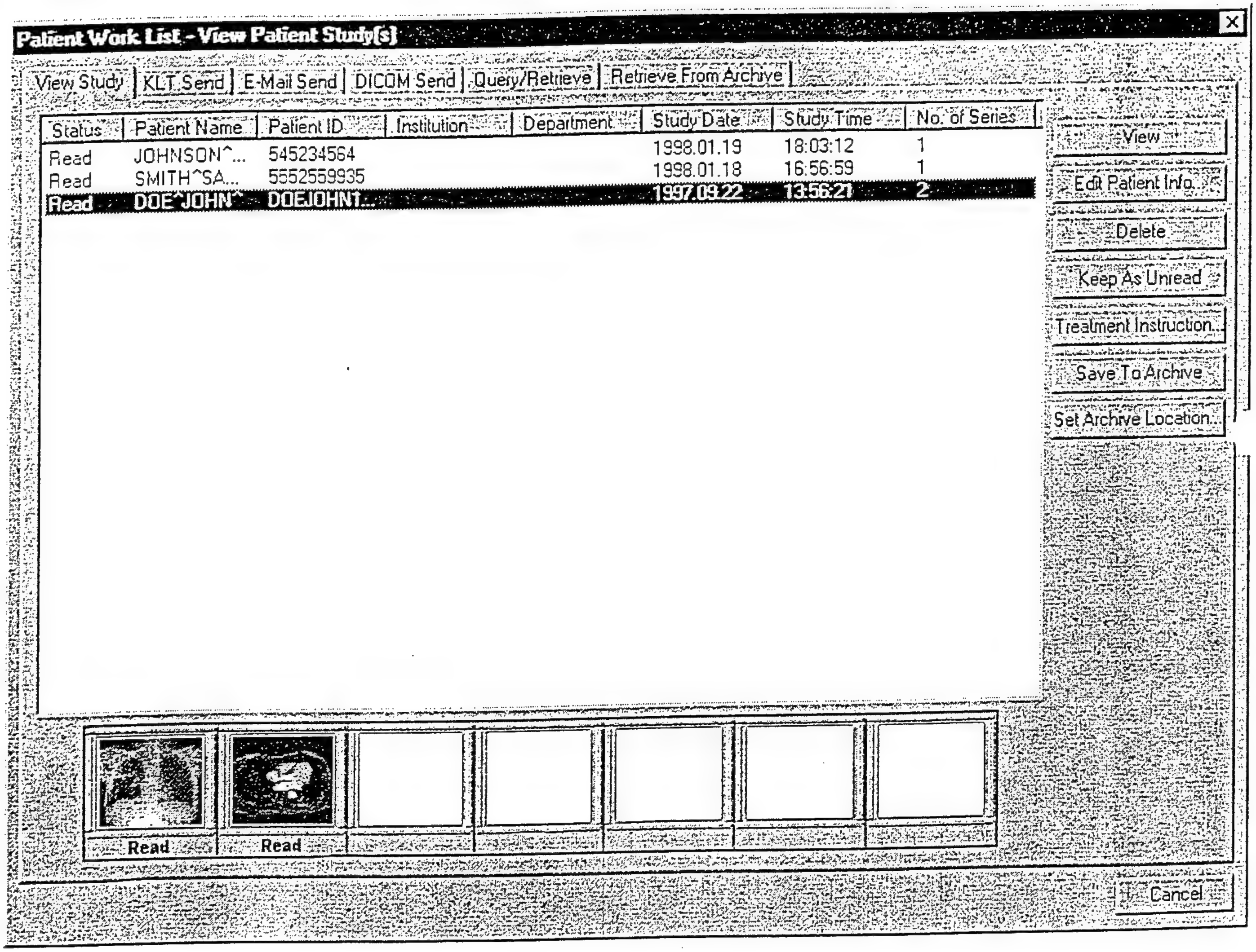


VIEWSEND Medical
File Dialer Edit Display Overlays Tools Setup Layout Window Help
DOE JOHN - 99220001.1: x=741 y=55 val=889
DOE JOHN
DOEJOHN1997092213562 1
G
Tools
56%
Study
19970922
Ready

One or more Series, each containing an image (or a sequence of images depending on the modality used) are stored in patient study folders. The folder is ideally suited for receiving downloaded images and records from a main archival storage system and there are several ways to create a new study.

While not intended as a long-term storage media for all patient image data, the VIEWSEND Medical system is only limited by the capacity of the storage media available to the PC. A limited amount of textual information is also stored with each study and is entered using the Study Folder Information form.

Patient Work List



Status	Patient Name	Patient ID	Institution	Department	Study Date	Study Time	No. of Series
Read	JOHNSON^...	545234564			1998.01.19	18:03:12	1
Read	SMITH^SA...	5552559935			1998.01.18	16:56:59	1
Read	DOE^JOHN^	DOEJOHNT...			1997.09.22	13:56:21	2

The Patient Work List shows a list of all studies available. The Patient Work List serves as a defacto home base, or starting point, for viewing, administering and sending patient information. It is the only place where:

- A study or a series within a study can be deleted
- Treatment Instructions can be created, modified or printed.
- A study can be sent to someone else using one of three methods (KLT Send, DICOM Send or E-Mail Send)

Study Status

The Study Status provides information related to how the Series in the study have been used. A single status indicator is used to collectively represent ALL Series Status indicators. Since each series status is independent of others series in the same study some rules apply governing which of these independent status' will prevail as the overall Study Status

- **No Status** – Used when there is a mix of series status indicators and no transmission failures have occurred for any series

- *Read* – Used when ALL series have been read and no transmission failures have occurred for any series
- **Unread** – Used if ANY series has not been viewed and no transmission failures have occurred for any series
- **Queued** – Used if ALL series is awaiting transmission by a KLT Send, DICOM Send or E-mail Send process

- *Sent* – Used when ALL series were successfully sent to at least one other location
- *Failed* – Used if an error was encountered during a send process and ANY series was not sent

Delete Study or Series

The same delete button is used to delete both a study and a series. From the Patient Work List:

To Delete a study:

Single-click the study name to highlight it, then click the "Delete" button. Click the "OK" button to confirm that you want to delete this study.

To Delete a Series:

Single-click a study, then single click the thumbnail image of the series to be removed to highlight it. Click the "Delete" button. Click the "OK" button to confirm that you want to delete this series.

Archiving Study Information

Allows outdated patient images (studies) to be saved and stored external to the PC. While it certainly could be used as a simple image storage database, VIEWSEND Medical was not intended for this purpose. In normal use, an image will be captured, sent and, upon confirmation of receipt, archived or deleted.

All Archive actions are initiated from the Patient Work List screen.

Set Archive Location

1. Highlight (single-click) the desired study to archive
2. Click the '*Set Archive Location'* Button
3. Navigate through the Explorer-like window to designate the storage location

   Note:

   The idea behind archiving is to free space on the local PC hard drive. It is most likely, therefore, that a network drive or other external storage device/location will be selected.

Save To Archive

1. Highlight (single-click) the desired study to archive
2. Click the '*Save To Archive'* Button
3. Click the 'Yes' button to confirm the study is to be saved
4. Click 'Yes' in the next dialog box that appears to save the study and remove it from the current Patient Work List or click 'No' to make a copy of the study in the archive and leave the original in the current Patient Work List

   Note:

   If the study already exists in the archive, you will be asked if you want to overwrite it.

Retrieve From Archive

1. Click the '*Retrieve From Archive'* Tab
2. Click the 'Select Source' button and navigate through the Explorer-like window to designate the storage location
3. Click the 'Load Archive' button to display all studies in the archive
4. Select desired study(s) to be retrieved using Windows conventions (Ctrl key for multiple selections) and click the '*Retrieve Selection(s)* button.

Delete From Archive

1. Follow steps 1 through 3 under '*Retrieve From Archive'*.
2. Select desired study(s) to be deleted using Windows conventions (Ctrl key for multiple selections) and click the '*Delete Selection(s)* button.

Creating a Series Report

Gives detailed information about a given series within a study, including selected thumbnail image(s). Information about the study is also included with the report.

Main Menu – File – Create Series Report or ▤

1. Open a study and open the desired series in the working window.
2. Bring up Series Report creation form by either going through the menu path above or clicking the Toolbar Icon shown.

3. Fill-in all required information as indicated by an ** next to the field name.

4. Select image(s) to include in the report.

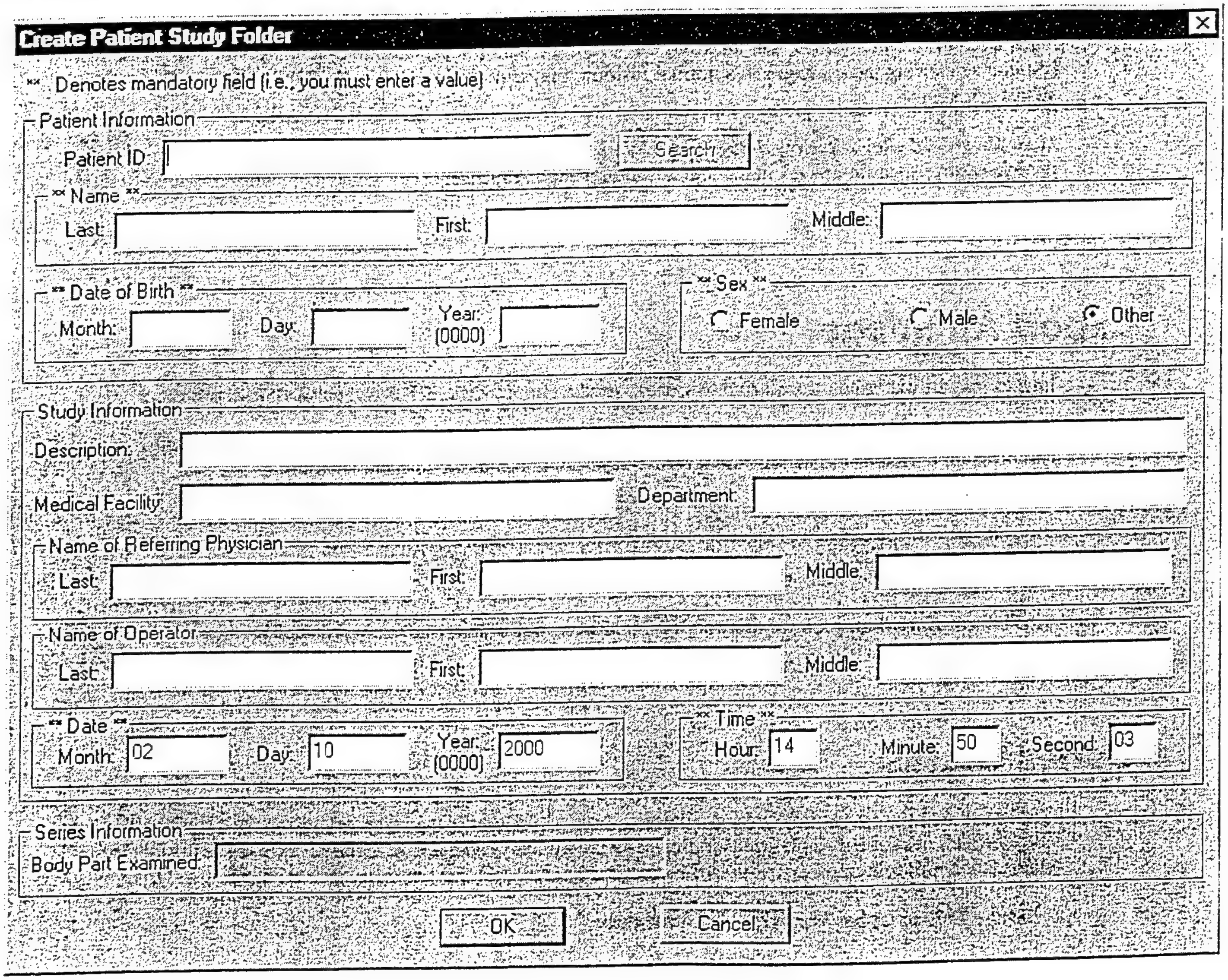
   Note:

   If the series is multi-image DICOM 3.0. up to 5 images may be selected using the slider control next to the picture box or by entering the image sequence number below the slider control.

5. Enter comments below the thumbnail view(s)

6. Click the Print or Print Preview button

Study Folder Information



Create Patient Study Folder

** Denotes mandatory field (i.e., you must enter a value)

Sex: ○ Female ○ Male ● Other

Date: Month: 02 Day: 10 Year: (0000) 2000

Time: Hour: 14 Minute: 50 Second: 03

4) Press down on the left mouse button to start one end or the anchor point of the ellipse.

5) Move the mouse with the left mouse button is still depressed.

A flexible ellipse stretches from the anchor point to the mouse position.

6) Release the left mouse button to complete the ellipse.

Tool Palette - Flip/Rotate

Rotate clockwise/counter-clockwise tools and

Flip vertical/horizontal tools

Used to change the image to an orientation with which the viewer is comfortable. This allows the original image to be scanned *once* in any direction, yet server the tastes of many viewers.

Tool Palette - Freehand

Draws a freeform shape in the graphics window.

To Draw

1) Optionally, select a color and a pen size tool in the tool palette. The default color is yellow and the default size is one.

When you first start a VIEWSEND Medical application and each time you connect to a remote site, the color and size tool are defaulted to yellow and 3, respectively.

2) Click on in the tool palette.

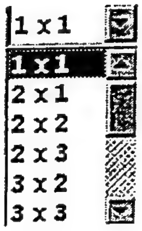
3) Move the mouse into the graphics window's drawing area.

4) Click and hold the left mouse button.

5) Begin drawing freehand shapes with the left mouse button is still depressed.

6) Release the left mouse button to finish the drawing.

Tool Palette - Image Layout Option



Used when viewing a series containing Dicom 3.0 multiple images in the Stack Mode. Controls the number of images that appear in the viewing window without scrolling and the position of those images.

Tool Palette - Invert

The invert tool changes the default negative image into a positive image, or visa-versa. Negative images are preferred in the US, while positive images are standard in Europe.

Tool Palette - Magnifier

Multiplies the current magnification factor of an image by 2X .

To Enlarge the View of an Area

1. Optionally, select a color tool and a size tool from the tool palette.

   When you first start VIEWSEND Medical and each time you connect to a remote site, the color tool and size tool is defaulted to yellow and 3, respectively.

2. Click on in the tool palette.

   When you first start VIEWSEND Medical and each time you connect to a remote site, the drawing tool is defaulted to the Neutral tool.

3. Move the mouse into the graphics window's drawing area.

4. Press the left mouse button down on the spot to be magnified.

   The border of the bounding square reflects the color that is currently selected in the color tool. Furthermore, the size of the magnification area is dependent on the size of size tool selected.

5. Release the left mouse button to stop magnifying.

Tool Palette - Mover

If the graphic image is larger than the window the hand can be selected to move the image around within the window.

Tool Palette - Neutral Tool

Cancels the operation of other tools in the Tool Palette.

The neutral tool is 1) an indicator for the location of the mouse pointer, 2) allows selection of other tools and windows and 3) switches between the tile and stack modes if the user double-clicks the left mouse button when viewing a multi-image series.

Tool Palette - Pen Color

Sets the color of the current selected drawing tool.

To Set the Color of a Drawing Tool

Click on one of the colors in the VIEWSEND Medical tool palette (the default color is yellow).

Drawing tools affected by the color tool are: Freehand, Ellipse, Rectangle, Text, Caliper, Angle and Profile

Tool Palette - Pointer

Enlarged pointer used to call attention to any area in the graphics window. Helpful in the full VIEWSEND Medical product for real-time collaboration with a distant site (the pointer is white on the local screen and red on the far-end). The pointer is valuable in VIEWSEND Medical for local consultation when all parties are viewing the same monitor.

To Use the Pointer

1) Click on in the tool palette.

   When you first start VIEWSEND Medical and each time you connect to a remote site, the drawing tool is defaulted to the Neutral tool.

2) Move the mouse into the graphics window's drawing area.

3) Click and hold the left mouse button to display the enlarged arrowt.

4) Release the left mouse button to stop using the pointer.

Tool Palette - Polygon

Used to draw a polygon shape using the selected line size and color.

1) Optionally, select a color tool and a size tool from the tool palette.

   When you first start VIEWSEND Medical and each time you connect to a remote site, the color tool and size tool is defaulted to yellow and 3, respectively.

2) Click on in the tool palette.

   When you first start VIEWSEND Medical and each time you connect to a remote site, the drawing tool is defaulted to the Neutral tool.

3) Move the mouse into the graphics window's drawing area.

4) Click the left mouse button to begin drawing.

5) Move the mouse to another spot and left mouse click to extend the line to that spot (repeat for each line segment desired.

6) Double-click the starting point to end the drawing

Tool Palette - Profile

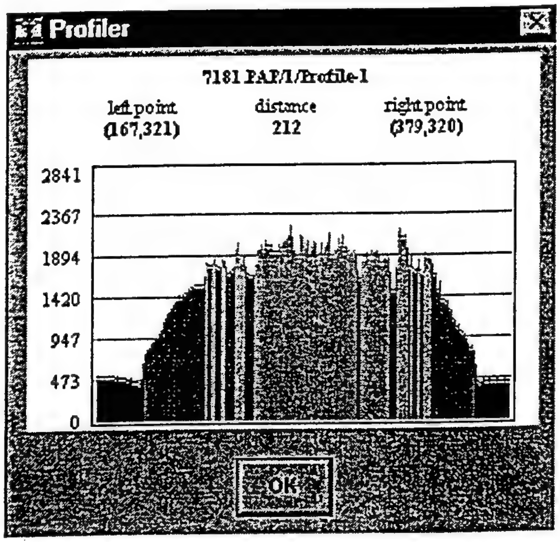
Plots a histogram of intensity levels along a selected line drawn on a medical image.

1) Click on ▨ in the tool palette.

2) Draw a line between any two points within a medical image.

3) From *Main Menu - Overlay* choose *Show Graph* to view the histogram.

A typical histogram is shown here.



7181 PAP/1/Profile-1

left point (167,321)

distance 212

right point (379,320)

Tool Palette - Rectangle

Draws a rectangle or square in a VIEWSEND Medical graphics window.

To Draw a Rectangle

1) Optionally, select a color tool ▨▨▨▨▨▨ and a size tool ▨▨▨▨ from the tool palette.

When you first start VIEWSEND Medical and each time you connect to a remote site, the color tool and size tool is defaulted to yellow and 3, respectively.

2) Click on ▨ in the tool palette.

When you first start VIEWSEND Medical and each time you connect to a remote site, the drawing tool is defaulted to the Neutral tool.

3) Move the mouse into the graphics window's drawing area.

4) Click and hold the left mouse button to start one end of the rectangle (the anchor point).

5) Move the mouse with the left button still depressed.

   A rubber-band rectangle stretches from the anchor point to the mouse position.

6) Release the left mouse button to complete the rectangle.

Tool Palette - Sizing

Sets the size of the current selected drawing tool. There are four different sizes; 1 is the smallest,4 the largest.

To Set the Size of a Drawing Tool

Click on one of the sizes from in the VIEWSEND Medical tool palette (default size is one).

Drawing tools affected by the size tool are: : Freehand, Ellipse, Rectangle, Text, Caliper, Angle and Profile

Tool Palette - Stack

This tool stacks Dicom 3.0 multiple images on top of each other in a single display window according to the Image Layout Option. During animation individual images are brought to the top of the stack.

Tool Palette - Text

Enters text in VIEWSEND Medical graphics window.

1) Optionally, select a color tool and a size tool from the tool palette.

   When you first start VIEWSEND Medical and each time you connect to a remote site, the color tool and size tool is defaulted to yellow and 3, respectively.

2) Click on in the tool palette.

   When you first start VIEWSEND Medical and each time you connect to a remote site, the drawing tool is defaulted to the Neutral tool.

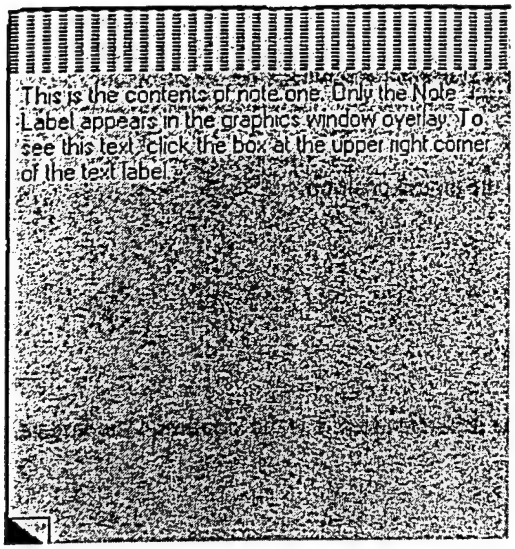
3) Move the mouse into the graphics window's drawing area.

4) Click the left mouse button where you want to enter the text and begin typing.

   Text cannot be entered beyond the right edge of the graphics window or the scrollbar.

5) Only the text label will appear on the graphics window overlay. To see full note text, select the Neutral Tool then left-mouse click on the large box in the upper right corner of the text label Note One.

6) Click anywhere in the resulting display box to hide it again.



This is the contents of note one. Only the Note Label appears in the graphics window overlay. To see this text, click the box at the upper right corner of the text label.

Tool Palette - Tile

This tool displays Dicom 3.0 multiple images in a matrix arrangement. The largest number of images possible are displayed on the screen simultaneously.

Tool Palette - Wiper

The Wiper tool removes ALL annotations from the VIEWSEND Medical graphics window with one click. It does not remove any DICOM header overlay information.

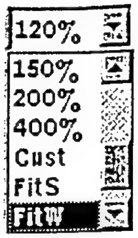
Tool Palette - Zoom In

The Zoom-In tool Increases the magnification factor. The arrows in the icon are pointing away from the center to indicate that the image is expanding, or getting larger.

Magnification factors available through the Zoom Option Control are 5, 10, 30, 50, 75, 100, 150, 200, 400 and 500 percent.

Tool Palette - Zoom Option

Changes the magnification of an image in the graphics window.



To use the Zoom Control Option click on the down arrow and select a magnification factor.

- Standard zoom factors are incremented up to 400 percent.
- Custom selects any other zoom factor with a maximum value of 500%.
- FitS sizes the image proportionally to the whole screen
- FitW fits the image porportionately to the current window size.

Tool Palette - Zoom Out

The Zoom-Out tool decreases the magnification factor. The arrows in the icon are pointing toward the center to indicate that the image is collapsing, or getting smaller.

Magnification factors available through the Zoom Option Control are 5, 10, 30, 50, 75, 100, 150, 200, 400 and 500 percent.

Overlays & Graphs

Overlay

Annotations of all types (notes, lines, ellipse, etc.) made on an image are maintained in a transparent overlay. The overlay can be manipulated independently from the image. For example, it is possible to temporarily Hide the Overlay (*Main Menu – Overlay – Hide Overlays*), Show it again (*Main Menu – Overlay – Show Overlays*) or clear all annotations from the overlay in a single click either through the *Main Menu – Overlay – Clear Overlays* command or by clicking the Wiper Tool on the tool palette.

Note:

DICOM 3.0 images usually display textual information in the upper left corner of the image(s). Because this information is an integral part of the image file, overlay actions do not affect it and it will always be in view.

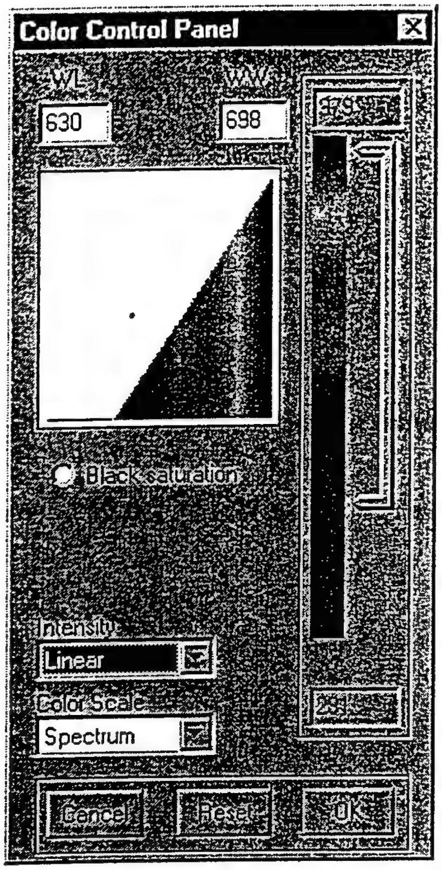
Graphs & Charts

There are two tools on the Tool Palette that have graphs underlying their overlay annotation. The Profile Tool has a graph that shows the density of the image along the line and the Freehand Tool graph shows the area falling within a closed freehand shape (the end point is co-located with the beginning point).

Image Appearance

Adjusting Colors

Accessed through *Main Menu – Display – Adjust Colors*



Color Control Panel

WL 630

WW 698

○ Black saturation

Intensity: Linear

Color Scale: Spectrum

Special features provided by this panel include: The control of black saturation that allows pixels that have a higher intensity than the maximum intensity selected to be colored black; The selection of different intensity settings, and the addition of false color.

The Color Panel Window provides the additional ability to select intensity types other than linear, such as exponential, logarithmic and sigmoid.

These intensity types settings are pre-defined and are provided with the software. Other intensity types can be user defined using look-up tables. The exponential, logarithmic and sigmoid intensity types are mathematically defined and their selection allows the further ability to control the slope of the curve using the slope control slider.

The Color Control Panel also provides for the selection of different standard scales (NIH, Hotiron, etc.) that can be used to false color medical images.

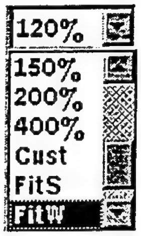
It is also possible to simply invert gray scale images.

Rotate, Flip & Zoom

- Rotate clockwise/counter-clockwise tools and
- Flip vertical/horizontal tools

  Used to change the image to an orientation with which the viewer is comfortable. This allows the original image to be scanned *once* in any direction, yet server the tastes of many viewers.

- The Zoom-In tool Increases the magnification factor. The arrows in the icon are pointing away from the center to indicate that the image is expanding, or getting larger.
- The Zoom-Out tool decreases the magnification factor. The arrows in the icon are pointing toward the center to indicate that the image is collapsing, or getting smaller.
- The Zoom Option Control Changes the magnification of an image in the graphics window.



To use the Zoom Control Option click on the down arrow and select a magnification factor.

- Standard zoom factors are incremented up to 400 percent.
- Custom selects any other zoom factor with a maximum value of 500%.
- FitS sizes the image proportionally to the whole screen
- FitW fits the image porportionately to the current window size.

Displaying Coordinates

Main Menu – Display – Show Coordinates and *Main Menu – Display – Hide Coordinates*

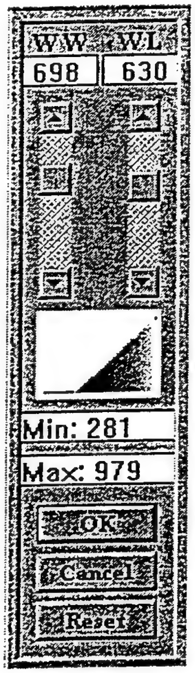
Displays X & Y cursor location and density value in the window title area.

Contrast & Brightness

The contrast control on the tool palette provides the means to visually adjust the contrast and brightness of the displayed image. All adjustments use the full dynamic range of the graphical image. For medical images, the dynamic range can be as low as 256 gray levels (8 bits) up to 65536 levels (16 bits). The dynamic range of some images may exceed the dynamic range of the intensities that can be displayed on a particular monitor. Typical computer workstation monitors are set to 256 levels. By using these adjustments the user can map the real dynamic range of the image to the displayed dynamic range.

It is necessary to be able to control the contrast and intensity of a medical image displayed on a monitor that has less dynamic range than is available in the image. When the medical image dynamic range equals the displayed dynamic range then contrast or intensity control is not useful. However, when the medical image has greater dynamic range than the display it is possible to enhance the displayed image to bring out medical image detail buried by the display. The contrast and intensity control allows the user to shift the complete dynamic range of the display to match a similar region of the medical image.

Contrast and intensity can be controlled by adjusting the vertical slider bars in the control.



WW	WL
698	630

Min: 281

Max: 979

The effect of adjusting the contrast and intensity can be seen in the Intensity Scale window and on the medical image. All active images are updated with the new intensity and contrast settings when the OK button is selected.

More precise control over contrast and intensity can be achieved by using the *Main Menu – Display - Adjust Color* command. Selecting this command brings up the Color Panel window.

Window Management

Window Manipulation

There are several *Main Menu* items that impact window management.

Main Menu - *Setup*

Disable Synchronization

This menu choice applies only when the *Main Menu – Setup – Preference Settings – Display* "Maximum Number of Image Windows Allowed Open" option is set to "Two Windows Only". This option pre-dated the multiple window option in current versions of VIEWSEND Medical software. The primary advantage of the two windows mode is that notations on the overlays of both windows can be synchronized (or not, using this menu item)

Main Menu - *Layout*

Find Image/Video/Tools/Study

This menu choice allows objects previously hidden from view to be re-displayed. For example, it is possible to drag the tool palette off the bottom edge of the screen and out of view.

Two Window/One Window

In the two-window only mode (See explanation above under Disable Synchronization) these menu choices and the toolbar icon ◫ allow alternating between a single window and two windows.

Goto Default

This option only applies to video windows directly under control of VIEWSEND Medical (does not include NetMeeting video windows). When selected, the video window will be re-displayed in its home position (upper right corner of screen) in its original size.

Main Menu – Window

The following sub-menu items are available:

Restore Image

In the *Main Menu – Setup – Preference Settings – Display Tab - Two-Window Only* mode, this option restores a minimized image window. Also note it is only possible to minimize an image window in the *Two Window Only* mode when the view is set to One Window. Minimization is not allowed when two windows are being viewed because synchronization is not possible.

Show Chat

Opens a chat window for exchanging textual message with others on the conference call. This feature will rarely be used and is primarily a diagnostic tool when the audio portion of the call is not working properly.

Hide/Show Image

Minimizes/Restores a window while in the Two Window Mode only.

Self View - Quarter/Half/Full

This option applies to the Zydacron Z240 codec only. It is the only codec to date that uses two video windows to display near-end and far-end video. Newer codecs use Picture in picture (PIP).

Cascade	Displays multiple images as a stack with upper left-hand corner of image window visible
Tile horizontally	Positions images and sizes all open images in a view with maximum viewable dimension in the horizontal axis.
Tile vertically	Positions images and sizes all open images in a view with maximum viewable dimension in the vertical axis.
Close All Medical Images	Closes all open studies

Videoconferencing

The videoconferencing (video and audio) functions in the Viewsend have been disabled to meet the US State Department's security protocol. If the procedural guidelines for clinical teleconsultation requires the use of the patient-to-physician face-to-face videoconferencing (and if security clearance have been issues for clinical use), then these functions are available on the system for immediate use.

Conferencing Configuration Utility

Main Menu – Setup – Conferencing Configurations

Conferencing configuration options are grouped under three tabs: *Audio*, *System* Options and *Camera Control Interface.*

Audio

There are two sections with the audio tab.

Default Audio Device - Allows a choice between Speaker type devices (i.e. speakerphone) and, a private type of device (Handset, headphone, etc.)

Microphone Input – identifies the microphone source (either desktop camera microphone or line-level audio input).

System Options

There are three sections under System Options:

User Information – Used to identify participants on the conference call

Automatically Answer Remote Conference Call – A check box to allow auto-answer of all non-modem calls received.

Pre-consultation Host Mode Information – These controls are used to add a layer of protection to the station when it receives images. To restrict access, a *Password* may be enabled. When someone attempts to send images to the PC, the sender will be prompted for a password before file transfer can occur. The percentage of hard disk space that can be used for incoming images can also be set.

Camera Control Interface

Model – Presents a list to choose the camera being used with this PC

Move Speed – Used to control the speed of the camera motor. This will vary based on the brand of the camera used.

Test Camera Control Interface – Again, depending on which camera is used, this button will be activated to allow testing camera controls from within the VIEWSEND Medical software.

NetMeeting Features

All of the NetMeeting features are accessed through the *Main Menu – Tools* pull down menu.

Where audio and video features are desired, but high quality hardware codec equipment (e.g. Zydacron, Vcon, etc.) is not installed on the PC, VIEWSEND takes full advantage of MS NetMeeting software. VIEWSEND totally controls NetMeeting behind the scenes so users don't need to learn how to use another program. All NetMeeting windows created by VIEWSEND Medical (for video, application sharing, chat, whiteboard, etc.) can be manipulated independently of the VIEWSEND Medical application itself, just as though NetMeeting was started directly by the user.

Application Sharing

Once a conference call has been established, this feature allows sharing an application with others on the call. The process is simple. Start the application to be shared in the normal way. To begin sharing, Click *Main Menu – Tools – Application Sharing* and select the application from the displayed list.

There are a couple of issues to consider when sharing applications. The first is that it is inadvisable to share the VIEWSEND Medical application itself, even though it appears as a choice on the displayed list. There is also a behavior of NetMeeting that users new to sharing find confusing. Any objects on the local PC screen that are displayed ON TOP of is application being shared will appear as pattern filled boxes on the remote PC screens. For example, if an Excel spreadsheet is being shared and the PC that is sharing it has the video window displayed on top of the spreadsheet on the local screen, then the remote PCs will see a box in the same location on its screen. However the box on the remote screens(s) will not contain the video picture displayed on the local machine, but rather a box filled with a cross-hatched pattern. To avoid this, the Excel spreadsheet on the originating PC should be fully visible with no other windows or objects layered on top.

Collaboration

In addition to sharing the application, the originator can choose to allow the remote PC user to assume control over the application being shared. This is known as collaboration. To TAKE CONTROL of the application, a user simply double-clicks anywhere on the shared application window.

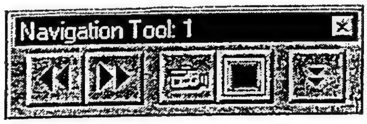
Upload Presentation and Presentation Mode

These features work together for the specific purpose of sharing a MS PowerPoint presentation.

Sending graphic images over a communications facility requires large bandwidth to make real-time simultaneous viewing practical. Under most circumstances, the NetMeeting call will not have the luxury of such capacity. For this reason, VIEWSEND Medical makes it possible, using *Main Menu – Tools - Upload Presentation*, to send the PowerPoint file to the remote station(s) that will be participating on the call in advance of the actual presentation. Because the remote site will then be running its own LOCAL COPY of the presentation, real-time slide changes are practical. The only remaining issue is keeping the locally running PowerPoint slide shows synchronized. That is the job of the *Main Menu – Tools - Presentation Mode* function.

In normal use, the presentation will be uploaded to the remote PC(s) just prior to the presentation. When the upload file transfer completes, VIEWSEND Medical will automatically go into the Presentation Mode. The screen that appears when the slide show is ready to proceed will vary depending on the video equipment and version of VIEWSEND Medical installed. Some hardware codecs (Zydacron 240+) will display the remote video in full-screen mode with the presentation *Navigation Tool* (see below) for controlling slide changes, etc. located in the lower right corner of the screen. On most PCs, however, after the PowerPoint file has been uploaded, a blank screen will appear with the presentation *Navigation Tool* located in the lower right corner of the screen. To begin the presentation, click the *Navigation Tool - Bring Slide Forward* button.

There is one more aspect of NetMeeting Presentation features that should be explained. When a PowerPoint file is uploaded, the file is given a special name by VIEWSEND Medical and saved on all PCs. This is a benefit in several ways. First, if the communications facility fails, the presentation can be resumed after the call is re-established without uploading the file again. This is accomplished by selecting *Main Menu – Tools – Presentation Mode* after the new call is set up. It also means that the PowerPoint file is always available until another one replaces it during another *Upload Presentation* process



Click any Navigation Tool button for more information

Whiteboard

Enabling this feature opens a window that contains a set of tools to allow simulating use of a whiteboard (chalkboard) in a real meeting room. Unlike a real meeting room whiteboard, work done in the NetMeeting whiteboard can be saved electronically for future use.

NetMtgNavTool - Exit

Exit Presentation Mode – Ends the slide show. At any time before another upload, the presentation can be re-started by selecting *Main Menu – Tools - Presentation Mode.*

NetMtgNavTool - FwdSlide

Bring Forward Slide – Show the PowerPoint presentation in full-screen mode. This means the video window (if available) will be hidden.

NetMtgNavTool - FwdVideo

Bring Forward Video - Show the full-screen remote video window on PCs equipped with a specific type of hardware codec. This means that the PowerPoint presentation will be hidden from view.

NetMtgNavTool - NextSlide

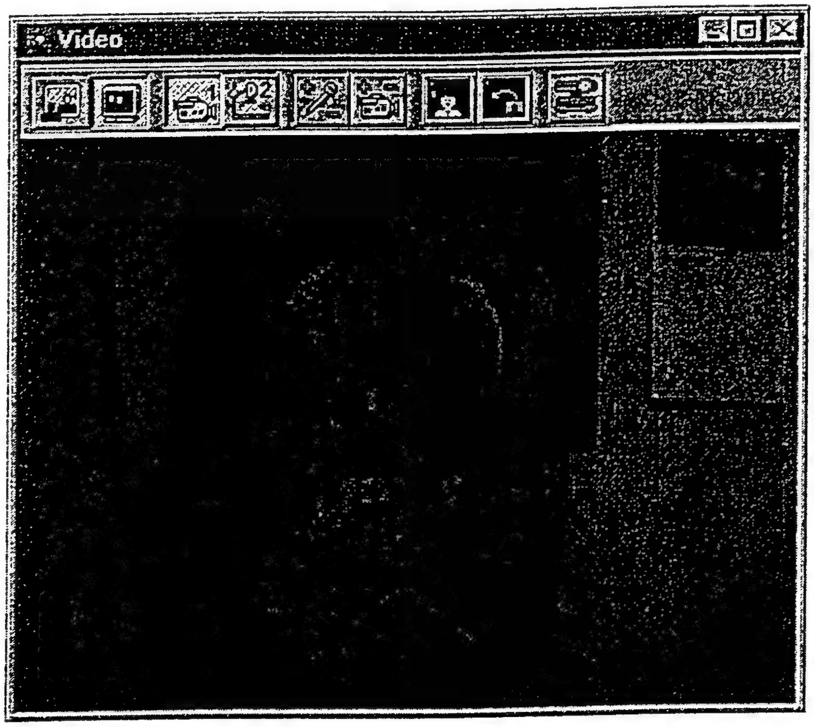
Show Next slide

NetMtgNavTool - PrevSide

Show Previous slide

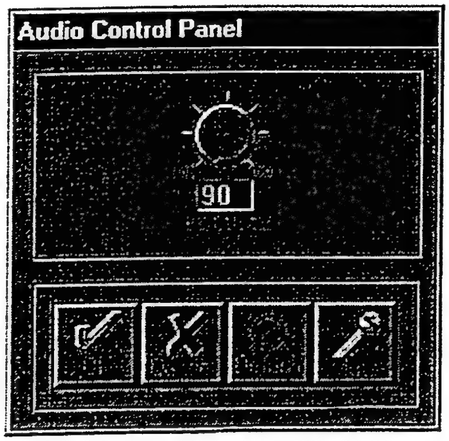
Video Window

Video Windows and camera controls will vary in appearance and content based on the PC equipment configuration. Some use multiple windows to display the local and remote pictures while others use Picture-In-Picture (PIP). Shown here are representative samples of video window components:



Click a Video Window Component for more information

Video Window - Audio Control Panel

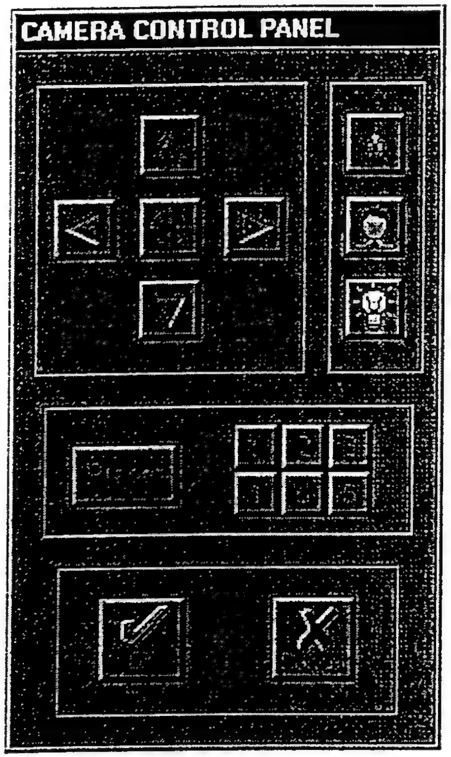


Control Functions are self-explanatory

Video Window - Backlight

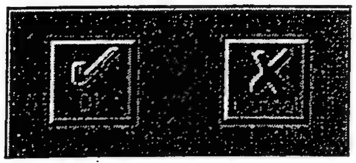
This particular video equipment contains a control that compensates for backlight (light emanating from behind the subject)

Video Window - Camera Controls



Click on a Camera Control for more information

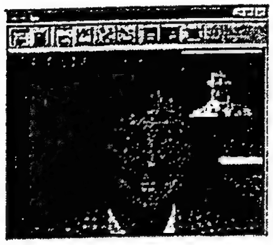
Video Window - OkCanx



The OK button accepts changes to video settings, while the Cancel button (in most equipment) will undo any changes made to settings during this session.

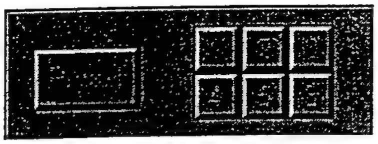
Video Window - PIP

The PIP On button activates the feature and displays a window similar to the one shown below. The larger picture is from the remote camera and the smaller one is from the local camera.



Two PIP control buttons will then be available. The left button will turn PIP Off and the right button will move the PIP (small) window to different locations within the larger picture. Some video equipment will allow the PIP to be dragged outside the larger picture where it is displayed in a window of its own.

Video Window - Presets



This particular video equipment allows six preset camera locations. To initialize a setting, the Preset button is clicked and the desired preset number is entered. Once set, simply clicking the preset number button moves the camera to that location.

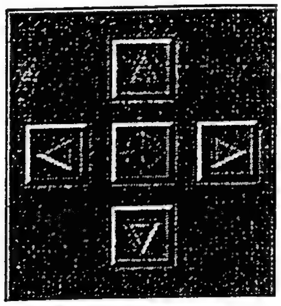
Video Window - RemoteView

Remote View – The large window will contain the image from the distant camera. This is the default setting.

Video Window - SelfView

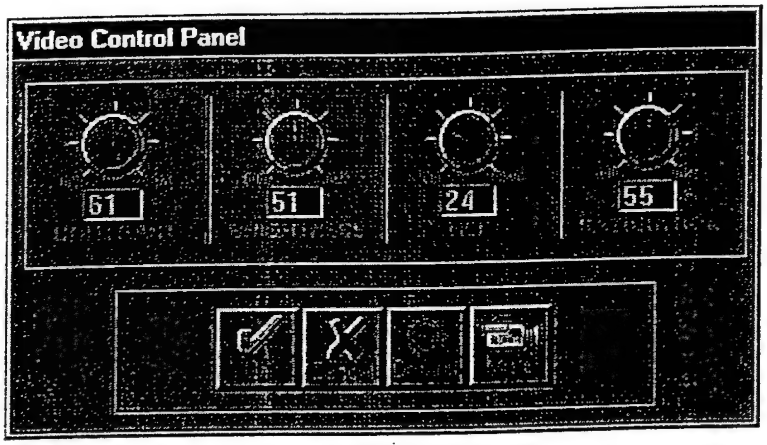
Self View – The large video window contains the image from the local camera. Ordinarily the video window contains the remote image.

Video Window - Tilt/Pan



Arrows control Tilt Up, Tilt Down, Pan Left and Pan Right actions. The button resets the camera to the factory default (usually pointing off to one side).

Video Window - Video Control Panel



Control Functions are self-explanatory

Video Window - Video Source

Most video equipment will provide more than one video source. In this example , a camera (source 1) and a document scanner (source 2) are depicted on the buttons. Actual devices controlled by these buttons will depend on the specific installation.

Video Window - Zoom

Two buttons are available for controlling camera Zoom, Zoom In and Zoom Out.

Printing Option

Main Menu – File - Print

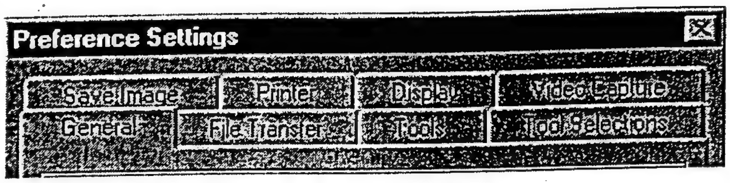
Printing is accomplished using the standard Windows print process. Use the Windows printer configuration utilities to manage the printer. If the DICOM print option has been purchased, additional capabilities are available for printing to film.

Main Menu – File - Page Setup

Used to set either the paper or film page characteristics

Preferences & Default Settings

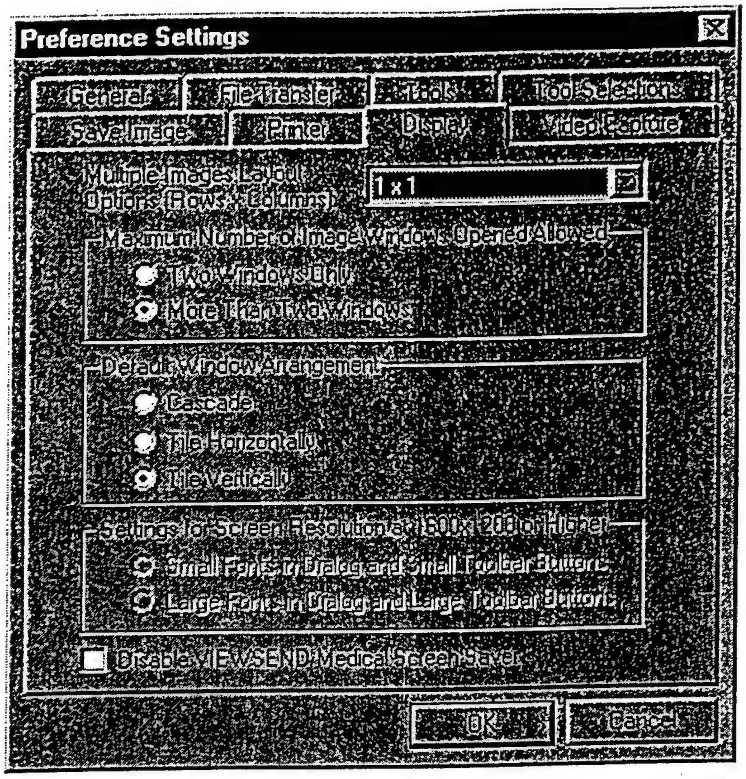
Preference Settings



Click any Preference Settings Tab for more information

Preference Settings - Display

Main Menu – Setup – Preference Settings - Display



Preference Settings

General | File Transfer | Tools | Tool Selections
Save Image | Printer | Display | Video Capture

Multiple Images Layout Options (Rows x Columns): 1 x 1

Maximum Number of Image Windows Opened Allowed
○ Two Windows Only
● More Than Two Windows

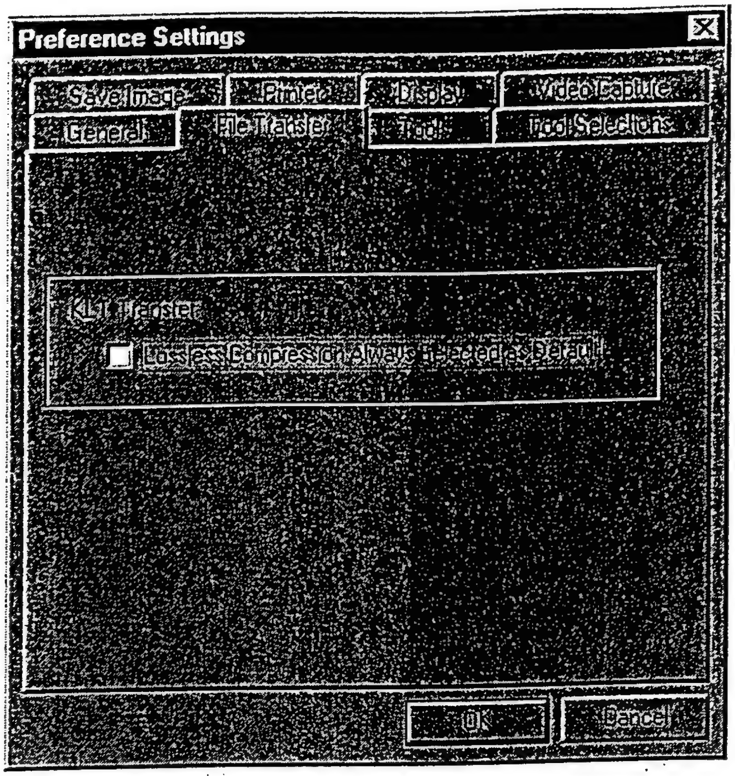
Default Window Arrangement
○ Cascade
○ Tile Horizontally
● Tile Vertically

Settings for Screen Resolution at 1600x1200 or Higher
● Small Fonts in Dialog and Small Toolbar Buttons
○ Large Fonts in Dialog and Large Toolbar Buttons

□ Disable VIEWSEND Medical Screen Saver

1. Used to choose either a two window or multi-window mode. (Two-Window mode offers auto-synchronized overlays between windows whereas multi-window allows unlimited number of simultaneous images)
2. Set default matrix (Image Layout Option) for viewing DICOM 3 multi-images in the `Stack Mode'
3. Set default Window arrangement (Cascade, Tile Vertical/Horizontal)
4. Turn the VIEWSEND Medical screen saver On/Off

Preference Settings - File Transfer



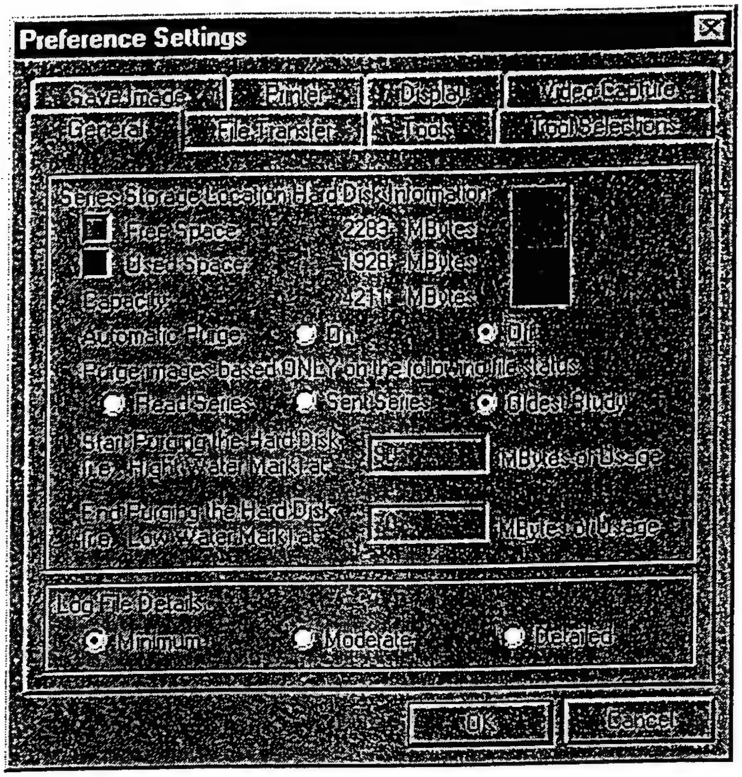
KLT Transfer

□ Lossless Compression Always Selected as Default

Allows setting lossless compression as the default for KLT proprietary file transfer operations.

Preference Settings - General

Main Menu – Setup – Preference Settings - General



Series Storage Location Hard Disk Information

□ Free Space 2283 MBytes

■ Used Space 1928 MBytes

Capacity 4211 MBytes

Automatic Purge ○ On ● Off

Purge images based ONLY on the following file status

○ Read Series ○ Sent Series ● Oldest Study

Start Purging the Hard Disk (i.e. High Water Mark) at [illegible] MBytes of Usage

End Purging the Hard Disk (i.e. Low Water Mark) at [illegible] MBytes of Usage

Log File Details

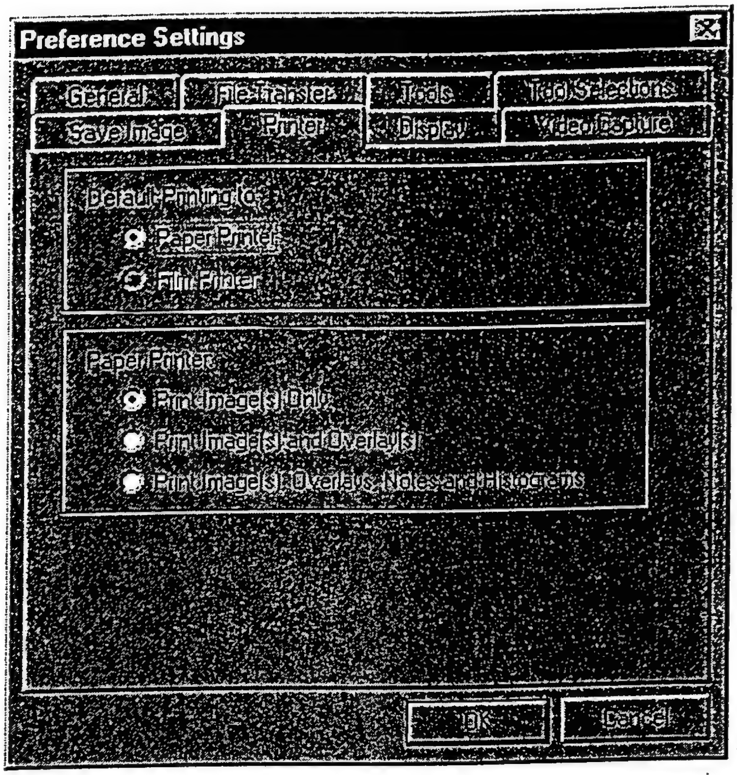
● Minimum ○ Moderate ○ Detailed

Provides a method for removing (purging) VIEWSEND Medical information from the hard drive where it is stored. (e.g. C:)

1. Thresholds are configurable for when the purge process should begin (High Water Mark – When the used disk space reaches this level) and when the purge process should stop (Low Water Mark – When the used disk space is reduced to this level).
2. Auto-purge can be set on/off
3. Selection of information to be purged can be based on Series Status (Read, Sent) or by Oldest Study
4. The level of detail captured in the purge log can also be set (Minimum, Moderate & Detailed)

Preference Settings - Printer

Main Menu – Setup – Preference Settings - Printer



Preference Settings

General | File Transfer | Tools | Tool Selections | Save Image | Printer | Display | Video Capture

Default Printing to:

● Paper Printer

○ Film Printer

Paper Printer

● Print Image(s) Only

○ Print Image(s) and Overlay(s)

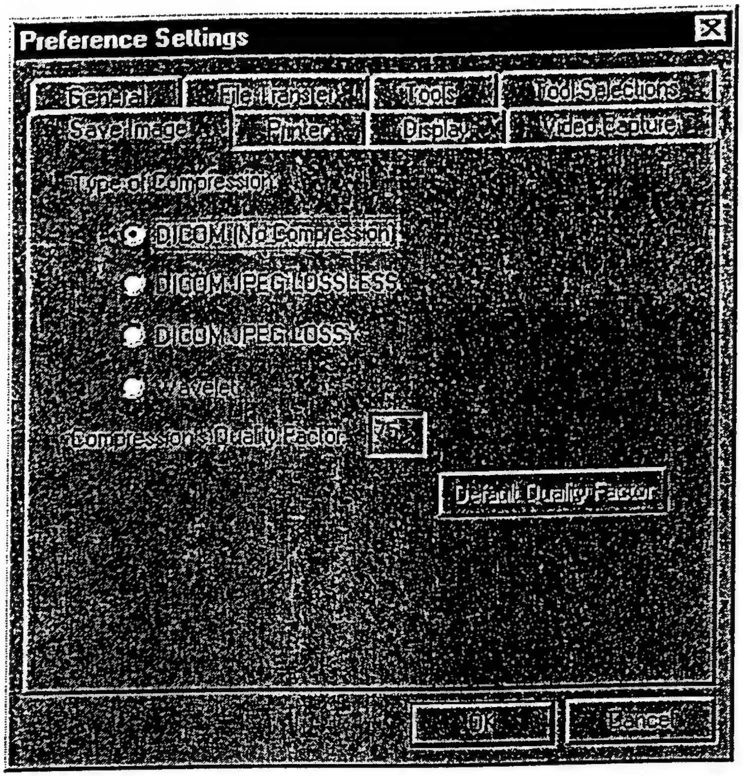
○ Print Image(s), Overlays, Notes and Histograms

OK | Cancel

Used to choose <u>where</u> to print (Paper or Film if DICOM option purchased) and <u>what</u> to print (image only, image with overlays, or image with overlays and graphs/charts underlying the notes on the overlay.

Preference Settings - Save Image

Main Menu – Setup – Preference Settings – Save Image



Type of Compression

● DICOM (No Compression)

○ DICOM JPEG LOSSLESS

○ DICOM JPEG LOSSY

○ Wavelet

Compression Quality Factor 75

Parameters for saving a new or modified image as a new series in a Patient Study Folder

TYPE OF COMPRESSION

Compression of medical images is desirable when bandwidth restrictions preclude a timely transmission of uncompressed images for collaborative consultation.

Warning:

Choices made here affect ALL images saved in the future. Once compressed, any information discarded is not recoverable, therefore the degree of loss and quality factor must be chosen carefully.

- DICOM (no compression)
- DICOM JPEG LOSSLESS (accepted by FDA as lossless compression methodology)
- DICOM JPEG Lossy (affected by Compression Quality factor)
- Wavelet (affected by Compression Quality factor)

QUALITY FACTOR

This number is a scalable compression quality factor.

Actual compression results will vary depending on the image being compressed.

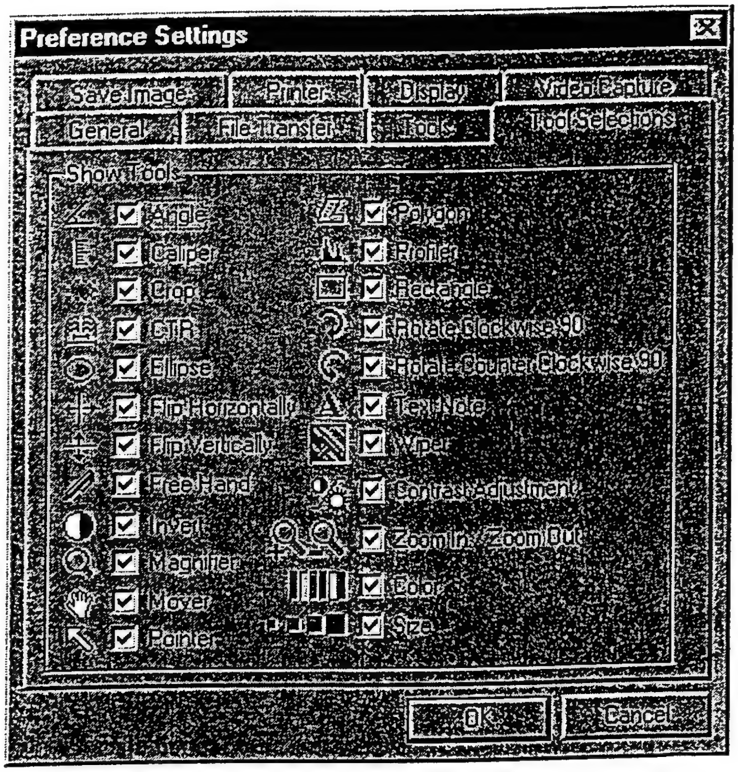
When a new compression quality factor is selected, an audit of the effected images is recommended to determine effectiveness and acceptability of the new setting.

With Wavelet compression, the LOWER the quality factor number, the lower the compression and the higher the quality.

With JPEG, the HIGHER the quality factor number, the lower the compression and the higher the image quality.

Preference Settings - Tool Selections

Main Menu – Setup – Preference Settings – Tool Selections



Show Tools

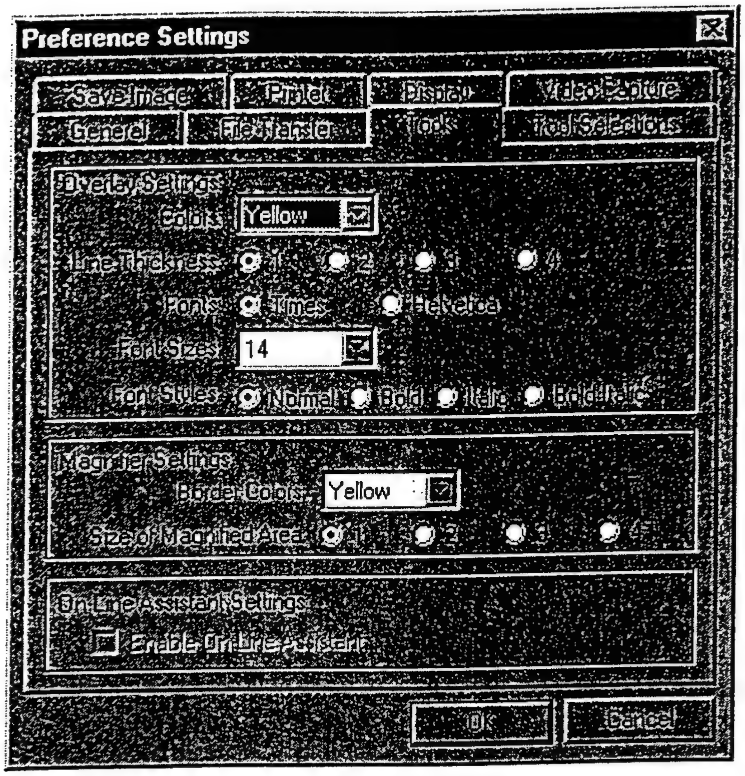
☑ Angle
☑ Caliper
☑ Crop
☑ CTR
☑ Ellipse
☑ Flip Horizontally
☑ Flip Vertically
☑ Free Hand
☑ Invert
☑ Magnifier
☑ Mover
☑ Pointer

☑ Polygon
☑ Profiler
☑ Rectangle
☑ Rotate Clockwise 90
☑ Rotate Counter Clockwise 90
☑ Text Note
☑ Wiper
☑ Contrast Adjustment
☑ Zoom In / Zoom Out
☑ Color
☑ Size

Used to choose which tools appear in the Tool Palette

Preference Settings - Tools

Main Menu – Setup – Preference Settings - Tools



Overlay Settings

Colors: Yellow

Line Thickness: ● 1 ○ 2 ○ 3 ○ 4

Fonts: ● Times ○ Helvetica

Font Sizes: 14

Font Styles: ● Normal ○ Bold ○ Italic ○ Bold Italic

Magnifier Settings

Border Colors: Yellow

Size of Magnified Area: ● 1 ○ 2 ○ 3 ○ 4

On-Line Assistant Settings

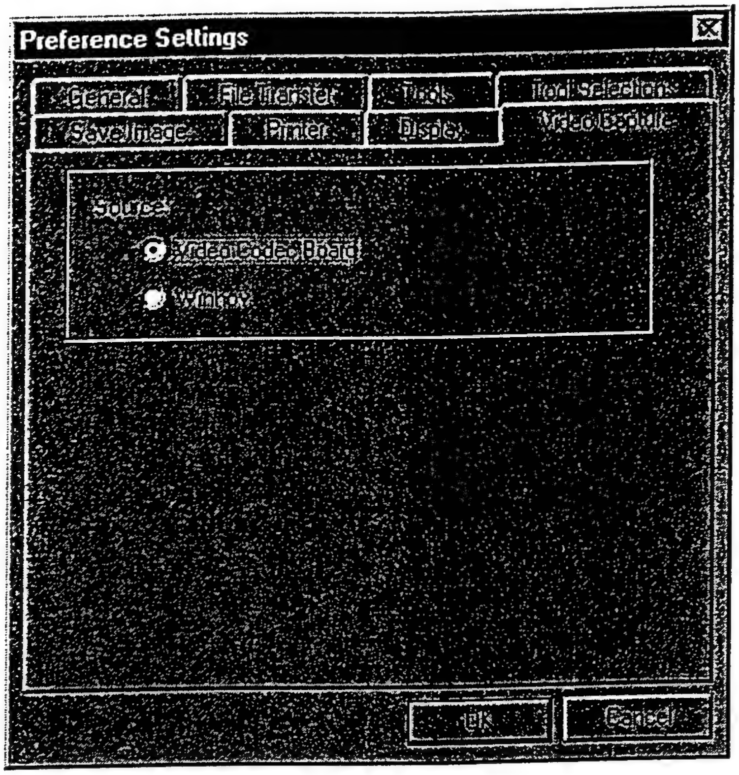
□ Enable On-Line Assistant

Used to set:

1. Overlay color, line and font properties for notations made on the image.
2. Magnifier properties
3. On-Line Assistant On/Off (RIX Only - Not applicable in VIEWSEND Medical)

Preference Settings - Video Capture

Main Menu – Setup – Preference Settings – Video Capture



Source:

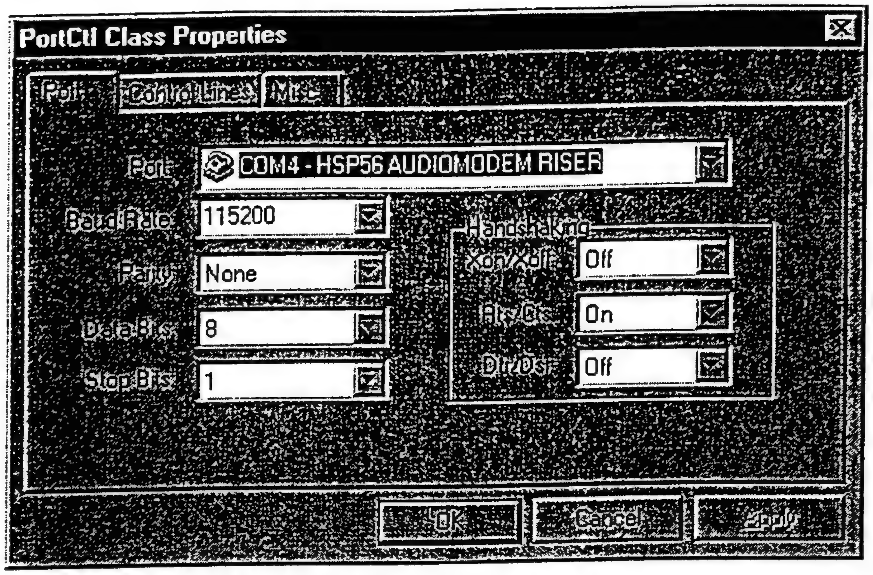
● Video Codec Board

○ Winnov

Choose a video capture method if the PC is equipped with either a WINOV video capture card or a Zydacron Codec

Modem Configuration

Main Menu – Setup – Modem Port Configuration



Port: COM4 - HSP56 AUDIOMODEM RISER

Baud Rate: 115200

Parity: None

Data Bits: 8

Stop Bits: 1

Xon/Xoff: Off

Rts/Cts: On

Dtr/Dsr: Off

Port Tab

Field	Function/Meaning
Port	Selects the modem or port for monitoring
Baud Rate	Selects the rate at which the computer will interface with the modem, (this is not the speed of the modem)
Parity	None - is default and appropriate for most uses
Data Bits	8 – is default and appropriate for most uses
Stop Bits	1— is default and appropriate for most uses
Handshaking : Xon/Xoff	Off -- is default and appropriate for most uses
Rts/Cts	On -- is default and appropriate for most uses
Dtr/Dsr	Off -- is default and appropriate for most uses

In normal use, the Port setting is the only item that must be set specifically for the PC in use. All other settings will work with defaults.

The Control and Misc. tabs are to be used only on the advise of technical support.

Dialing Properties

Main Menu – Setup – Dialing Properties

If your phone is provisioned with the call waiting feature, check the box in this option to disable the feature.

Call waiting will interfere with the transmission of data while VIEWSEND is receiving or sending a file

Station Information

Main Menu – Setup – Station Information

A form that optionally allows entry of information specific to image capture environment. The facility name and address, department and station name can be recorded. If a scanner is attached to the station, the manufacturer name, model and modality can also be entered.

Administrative Tasks

Logs

Menu Item	Sub-Menu Item	Function
Show Log		
	KLT Log	Displays (using MS WordPad) a log of activities. Normally, this log file is only used in conjunction with troubleshooting VIEWSEND Medical when assisted by technical personnel
	DICOM Log	Displays (using MS WordPad) a log of DICOM specific activities. Normally, this log file is only used in conjunction with troubleshooting VIEWSEND Medical when assisted by technical personnel
Delete Log		
	KLT Log	Deletes all entries in the KLT Log
	DICOM Log	Deletes all entries in the DICOM log

Reports

Series Report

There are several reports available in VIEWSEND Medical. The most valuable is a Series Report that gives detailed information about a given series within a study, including selected thumbnail image(s). Information about the study is also included with the report.

Treatment Instructions Report

Associated with each Patient Study Folder are Treatment Instructions. These instructions are accessed through a button on the Patient Work List and can be printed in a simplified report format.

Activity Reports (Received & Sent)

Both of these reports provide some basic statistics related to studies sent and received.

Database Integrity

Main Menu - Tools - Verify Database Integrity

Selecting this menu item will cause the active database to be re-indexed and will perform internal clean-up features on the database.

Run Diagnostics

This feature is limited to certain Zydacron codec models that make diagnostic functions available to VIEWSEND Medical Software.

Appendix G: Troubleshooting the Film Digitizer

Mike
I appreciate your follow up support. As per our Telephone conversation this morning I am forwarding the screen capture error I have received from Nairobi site. I would also appreciate if you ever get a chance to send the paint pro shop software that you promised to FedEx it 2 weeks ago. He said he has never received it. His mailing address is
U.S. Embassy Nairobi

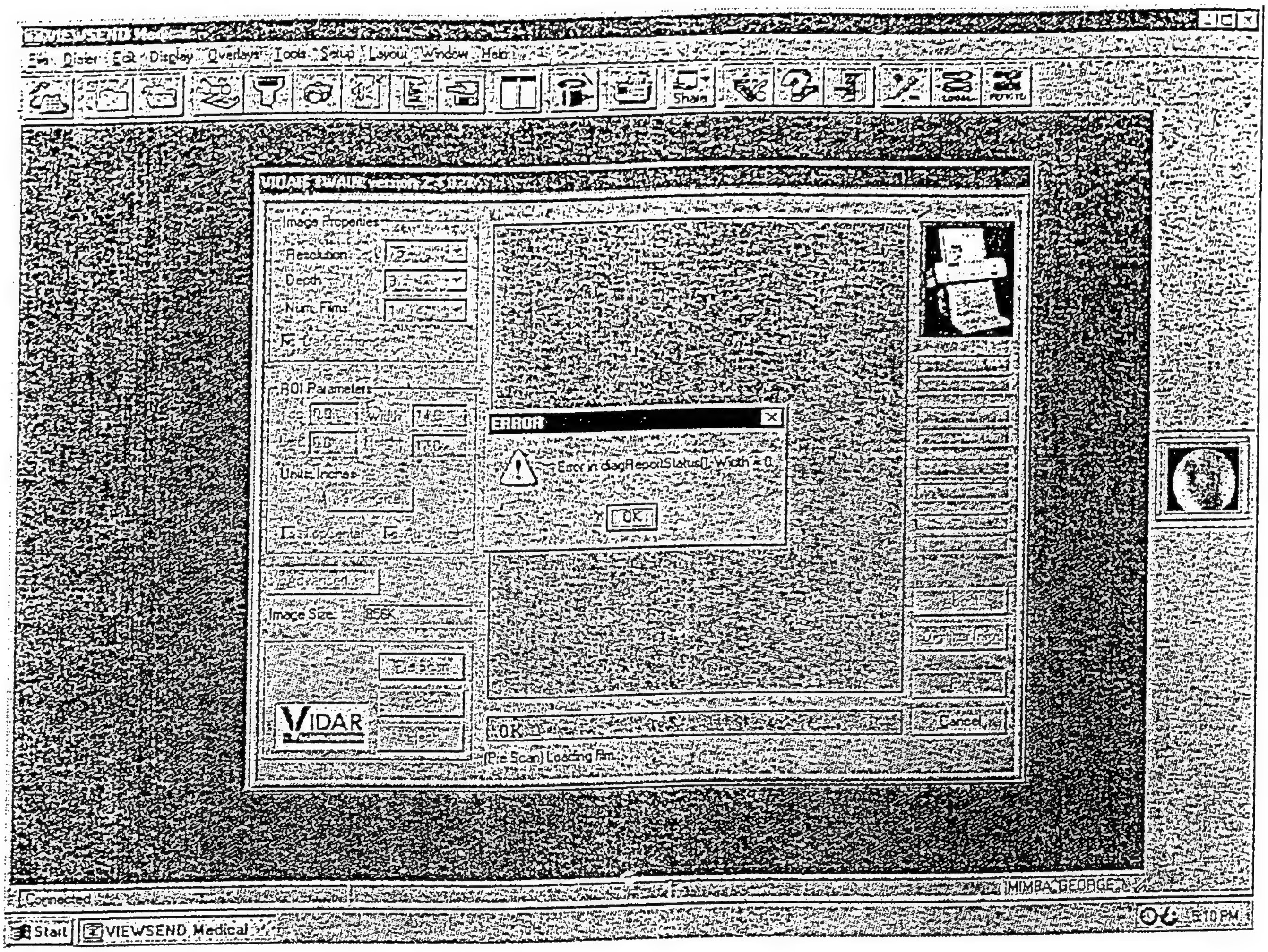
George M. Mimba
P.O.BOX 30137,
Nairobi Kenya
Tel: 011-254-2-537-800
Email: mimbagm@hotmail.com

Thanks for your continued support, I hope to hear from you soon.

Fikre Alemu
Telemedicine Technician
ISIS Center
Georgetown University
2115 Wisconsin Avenue, NW, Suite #603
Washington, DC 20007
Tel: (202) 687-0860 or 687-9110
Fax: (202) 784-3479
Email: Alemu@isis.imac.georgetown.edu
Web Page: http://www.isis.georgetown.edu

-----Original Message-----
From: VTC, Nairobi V [mailto:VTCNairobi@state.gov]
Sent: Tuesday, April 25, 2000 3:24 PM
To: 'nairobi@isis.imac.georgetown.edu'
Cc: 'khanafel@isis.imac.georgetown.edu'; 'alemu@isis.imac.georgetown.edu'; Teleconference, Med V
Subject: screen capture 1.doc*

* Screen capture sent as attachment for troubleshooting



ERROR

Error in diagReportStatus()- Width = 0.

OK

Image Size: 856K

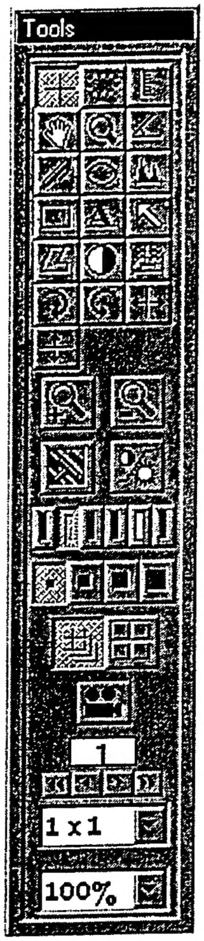
(Pre Scan) Loading Film...

Connected

MIMBA, GEORGE

- **Sent** – The series was successfully sent to at least one other location
- **Failed** – An error was encountered during a send process and the series was not sent

The Tool Palette



Click any Tool Palette button for more information!

The tool palette (and, independently, the thumbnail images) can be dragged to any location in the graphic window, or completely off the bottom edge of the screen. To move the Tool Palette, select the neutral tool, then click and hold the left mouse button on the Tool Palette border while dragging to the desired location.

Tool Palette - Angle

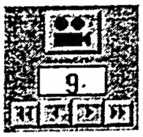
Measures an angle between two lines drawn on a medical image.

1) Click on ▨ in the tool palette.
2) Place the cursor at the angle apex, then click and release the left mouse button

3) Move the mouse to the end of the first line and click the left mouse button again.

4) Finally, move the cursor to the end of the second line to define an angle and click the left mouse button a third time. An angle will be drawn on the graphic using the pen color and pen size selected from the floating toolbar.

Tool Palette - Animate



These controls allow ALL images in a Dicom 3.0 multiple image series to be played in a 'movie' fashion, or advanced one image at a time.

When animation is in progress, This tool controls the sequence in which Dicom 3.0 multiple images are animated while This tool controls the speed in which Dicom 3.0 multiple images are animated.

Tool Palette - Caliper

Measures length in the VIEWSEND Medical graphics window.

To Measure a Distance

1) (optionally) Select a color and a size tool from the Tool Palette. (default color is yellow and size is one)

   When you first start a VIEWSEND Medical application and each time you connect to a remote site, the color and size tool are defaulted to yellow and 3, respectively.

2) Click on on the Tool Palette.

   When you first start a VIEWSEND Medical application and each time you connect to a remote site, the drawing tool is defaulted to Neutral.

3) Move the mouse into the graphics window's drawing area.

4) Click and hold the left mouse button to start one end of the line (anchor point).

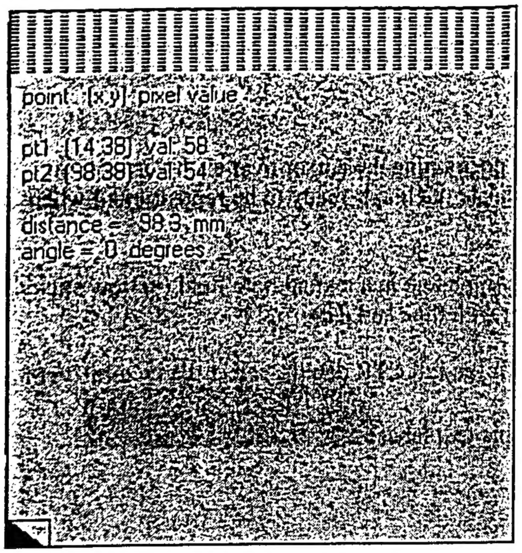
5) Move the mouse with the left mouse button still depressed.

   A flexible line stretches from the anchor point to the mouse position

6) Release the left mouse button to complete the line.

7) To see full details related to the line, select the Neutral Tool then left-mouse click on the large box in the upper right corner of the line measurement d = 98.3 mm.

8) Click anywhere in the resulting display box to hide it again.



point : (x,y) pixel value

pt1 (14,38) val 58
pt2 (98,38) val 54

distance = 98.3 mm
angle = 0 degrees

Tool Palette - Contrast

This tool ▨ is used to adjust contrast and brightness of the image. For a more detailed explanation of this complex topic, click here.

Tool Palette - Crop

▨ This tool allows selection of a specific region within a medical image for detailed examination. The cropped area becomes the total viewable image.

To crop a section of an image click and hold the left mouse button while dragging a box around the desired area. Release the mouse button to finish the selection. To complete the crop, click the right mouse button and choose "Crop" from the menu that appears. To un-crop, thereby restoring the original image, right-mouse click anywhere on the image and select "Uncrop" from the menu that appears.

Crop and Uncrop functions are also available from *Main Menu – Edit*. However, the Crop tool on the Tool Palette must still be used to first identify the image target area (dragging a box around the desired area).

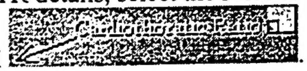
Tool Palette - CTR

The CTR tool is used to determine the Cardiothoratic Ratio in a chest x-ray.

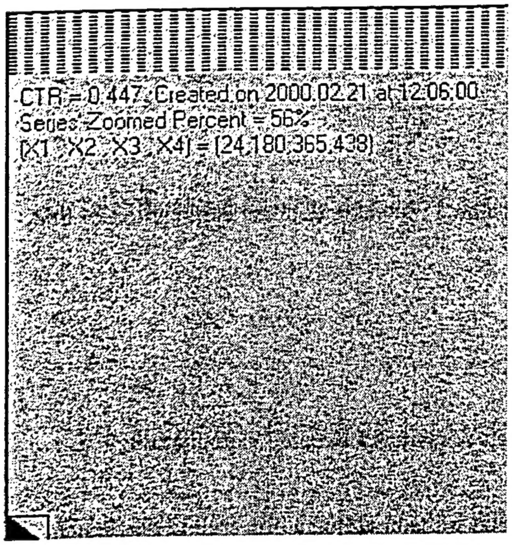
To take a CTR measurement

1) Align the vertical bars on either side of the chest/heart. Do this by positioning the cursor over each vertical line (the lines change color as the cursor is positioned over them to indicate the line is ready to be repositioned when the left mouse button is clicked).

2) Click the OK button (optionally, you may cancel) to record the measurement in a textual note field (yellow sticky.) Each successive CTR is appended to this same text note, annotated with time and date.

3) Only the CTR label will appear on the graphics window overlay. To see full CTR details, select the Neutral Tool then left-mouse click on the large box in the upper right corner of the text label .

4) Click anywhere in the resulting display box to hide it again.



CTR = 0.447, Created on 2000.02.21 at 12:06:00
Series Zoomed Percent = 56%
[X1 ,X2 ,X3 ,X4] = [24,180,365,438]

Tool Palette - Ellipse

Draws an ellipse in a VIEWSEND Medical graphics window.

1) Optionally, select a color and a pen size tool in the tool palette. The default color is yellow and the default size is one.

   When you first start a VIEWSEND Medical application and each time you connect to a remote site, the color and size tool are defaulted to yellow and 3, respectively.

2) Click on in the tool palette.

   When you first start a VIEWSEND Medical application and each time you connect to a remote site, the drawing tool is defaulted to Neutral.

3) Move the mouse into the graphics window's drawing area.